



User Manual

ECW/ECWO-Series Enterprise Access Point

Version 3.43.00

Table of Content

1.	Edgecore Enterprise Access Point Quick Deployment	3
1.1	Log in to the AP	3
1.2	General Information Configuration	5
1.3	Connect the AP to the Network	6
2.	Navigating the Web Management Interface	12
3.	System	13
3.1	General.....	13
3.2	Network Interface	15
3.3	DHCP Server.....	17
3.4	Management	18
3.5	CAPWAP	20
3.5.1	<i>To Manage by WLAN Controller with Complete Tunnel</i>	<i>21</i>
3.5.2	<i>To Manage by WLAN Controller with Split Tunnel</i>	<i>23</i>
3.6	IPv6.....	25
3.7	iBeacon (ECW5211-L, ECW5410-L, ECWO5211-L Only).....	25
3.8	RTLS (ECW5211-L, ECW5410-L, ECWO5211-L Only)	27
3.9	DPI DNS (ECW5211-L, ECW5410-L, ECWO5211-L Only)	27
4.	Wireless	28
4.1	VAP Overview	28
4.2	General.....	31
4.3	VAP Config	35
4.4	Security	37
4.5	Repeater	41
4.6	Advanced	42
4.7	Access Control	44
4.8	Hotspot 2.0	46
5.	Firewall	48
5.1	Firewall List	48
5.2	Service.....	52
5.3	Advanced	53
6.	Utilities.....	54
6.1	Change Password	54
6.2	Backup & Restore	55
6.3	System Upgrade	56
6.4	Reboot.....	57
6.5	Upload Certificate	57
6.6	Background Scan	58
6.7	Discovery Utility.....	59
6.8	Network Utilities.....	60

7.	Status	61
7.1	Overview	61
7.2	Interfaces	62
7.3	Associated Clients.....	62
7.4	DHCP Leases	64
7.5	Link Status.....	64
7.6	Event Log	65
7.7	Wireless Log.....	66
7.8	Monitor	67
8.	Console Interface	68
8.1	Direct Connection by Console Cables	68
8.2	Remote Connection by SSH Interface	69
9.	Hardware Overview	70

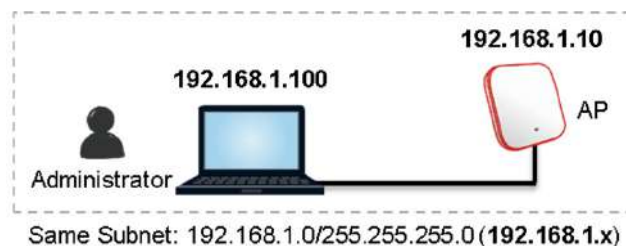
1. Edgecore Enterprise Access Point Quick Deployment

To set up The AP for the first time, administrators need to perform initial configuration to assign an IP address and other information necessary for the AP to communicate with the local gateways and for the AP to allow Wi-Fi devices to connect to the wired network.

1.1 Log in to the AP

The AP has a web-based interface for configuration and management. To access the Web Management Interface (WMI) for the first time, follow the steps below.

1. Ensure that your administrative PC is manually set to a static IP Address in the same subnet as the AP's (192.168.1.100/255.255.255.0). Connect the PC directly to the LAN port of the AP via an Ethernet cable.



2. Launch the web browser and enter the default IP Address of the AP (192.168.1.10) in the address field.




Log in using default Username (**admin**) and Password (**admin**) on the Administrator Login Page:

Diagram illustrating the Administrator Login Page. The page features the Edgecore logo at the top left. Below the logo, there are input fields for Username and Password, and a Login button. The background of the page shows a network diagram with nodes and connections.

3. **System Overview** page of the WMI will appear after login.

Home > Status > System Overview


System Overview


System

System Name	ECW5410-L
Firmware Version	3.43.00
Build Number	1.55-1.9293.2.21
Location	
Site	EN-A
Device Time	2000/01/01 23:22:23
System Up Time	0 days, 23:23:19
CPU/RAM Usage	3.13% / 34.93% Plot


Radio Status

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	A8:2B:B5:77:68:61	802.11g+n	6	18 dBm
RF Card B	A8:2B:B5:77:68:62	802.11ac	36	19 dBm



LAN Interface

MAC Address	A8:2B:B5:77:68:5F
IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Gateway	192.168.1.254



AP Status

RF Card Name : **RF Card A** ▼

Profile Name	BSSID	ESSID	Security Type	Online Clients	TUN
VAP-1	A8:2B:B5:77:68:61	Guest Network	Open	0	


CAPWAP


Status: **Disabled**



IPv6

Status: **Disabled**


4. Change the administrator's password for security reasons


- Click on the **Utilities** icon on the main menu, and select the **Change Password** tab.
- Enter the **New Password** and retype it in the **Re-enter New Password** field.


System


Wireless


Firewall


Utilities


Status

Change Password

[Backup & Restore](#)
[System Upgrade](#)
[Reboot](#)
[Upload Certificate](#)
[Background Scan](#)
[Discovery Utility](#)
[Network Utilities](#)

Home > Utilities > Change Password

Change Password

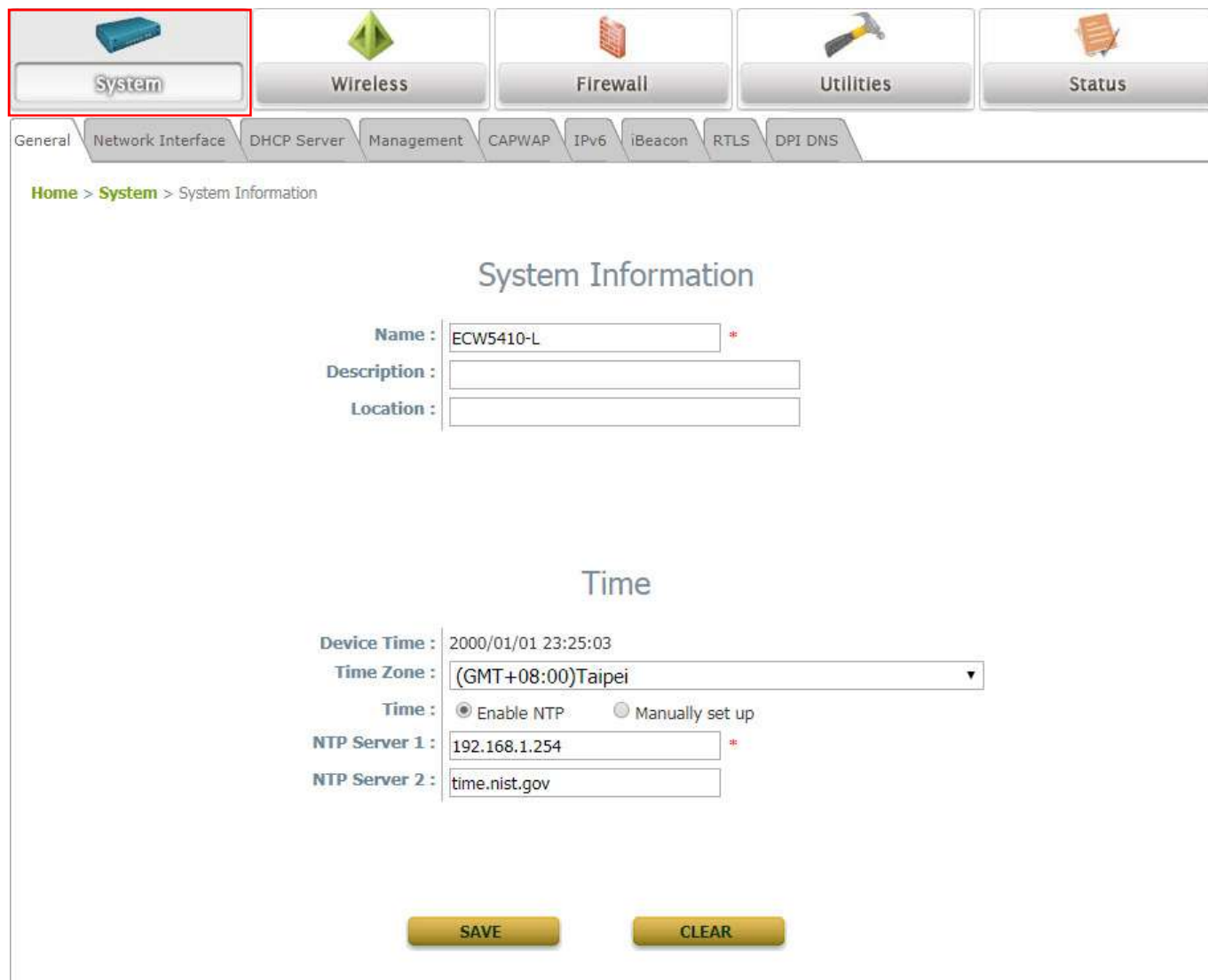
Name : **admin**
New Password : *up to 32 characters
Re-enter New Password :

Name : **user**
New Password : *up to 32 characters
Re-enter New Password :

SAVE
CLEAR

1.2 General Information Configuration

Go to System General page (Home > System > General) to configure general information for the AP.



General Network Interface DHCP Server Management CAPWAP IPv6 iBeacon RTLS DPI DNS

Home > System > System Information

System Information

Name : ECW5410-L *

Description :

Location :

Time

Device Time : 2000/01/01 23:25:03

Time Zone : (GMT+08:00)Taipei ▼

Time : ☒ Enable NTP ☐ Manually set up

NTP Server 1 : 192.168.1.254 *

NTP Server 2 : time.nist.gov

SAVE CLEAR

1. System Information: Enter appropriate system related information (**Name**, **Description**, and **Location**), by which administrators will be able to identify the AP in the network.

2. Time: For this initial configuration, set the system time for the AP using the method of **Enable NTP** (to sync the system clock with Network Time Protocol (NTP) server).

1.3 Connect the AP to the Network

The following instructions are the basic steps to establish the wireless coverage of your network. The AP will connect to the wired network through its LAN port and enable wireless access to your network.

Step 1: Change IP Settings of the AP

Go to **Network Interface** page (Home > System > Network Interface) to perform configuration of the network settings.

General Network Interface DHCP Server Management CAPWAP IPv6 iBeacon RTLS DPI DNS

Home > System > Network Settings

Network Settings

Mode : ☒ Static ☐ DHCP

IP Address : 192.168.1.10 *

Netmask : 255.255.255.0 *

Default Gateway : 192.168.1.254 *

Primary DNS Server : 192.168.1.254 *

Alternate DNS Server :

Ethernet IGMP Snooping : ☒ Disable ☐ Enable

Layer2 STP :

- Mode:
 - **Static:** Manually fill in appropriate values for the network interface (**IP Address**, **Netmask**, **Default Gateway**, and **Primary DNS Server**) – in the example above, the AP is still using the default IP address 192.168.1.10.
 - **DHCP:** If the deployment requires that the AP get a dynamic IP Address from the LAN, set Mode to **DHCP**; Click **SAVE** to submit the changes.

Step 2: Activate the first SSID for Wi-Fi access

By default, one Service Set Identifier (SSID) is enabled with the Radio A (**RF Card A**) and one SSID is enabled with the Radio B (**RF Card B**). As shown on the **VAP Overview** page (Home > Wireless > VAP Overview), Virtual Access Point No.1 (VAP-1) profile represents the first SSID available.

VAP Overview

RF Card A

VAP No.	ESSID	Network Mode	State	Security Type	MAC ACL	Hotspot 2.0
1	Guest Network	Bridge	Enabled	Open	Disabled	Disabled
2	Virtual Access Point 1	Bridge	Disabled	Open	Disabled	Disabled
3	Virtual Access Point 2	Bridge	Disabled	Open	Disabled	Disabled

Up to 16 VAPs

RF Card B

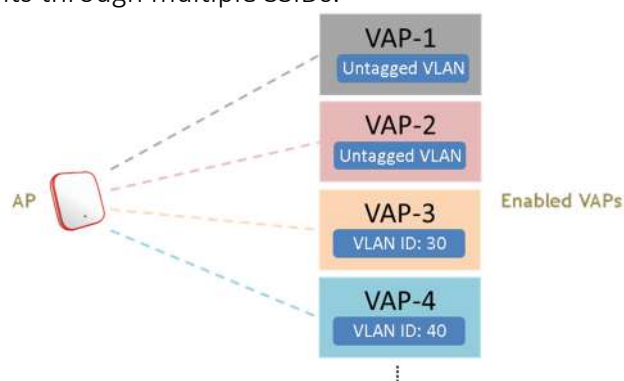
VAP No.	ESSID	Network Mode	State	Security Type	MAC ACL	Hotspot 2.0
1	Guest Network	Bridge	Enabled	Open	Disabled	Disabled
2	Virtual Access Point 1	Bridge	Disabled	Open	Disabled	Disabled
3	Virtual Access Point 2	Bridge	Disabled	Open	Disabled	Disabled

Up to 16 VAPs

Virtual Access Point (VAP):

- VAP feature allows a single physical AP device (with a unique, single BSSID) to present itself as multiple discrete APs, as shown in the example diagram below;
- Each VAP can be independently enabled or disabled, with its own settings (e.g. SSID, Network Mode, VLAN ID, Security, etc.), such that the AP is able to support different clients through multiple SSIDs.

►► Note:



Click on the State (**Enabled**) of VAP-1 to configure the profile. This will bring up the following VAP Configuration page.

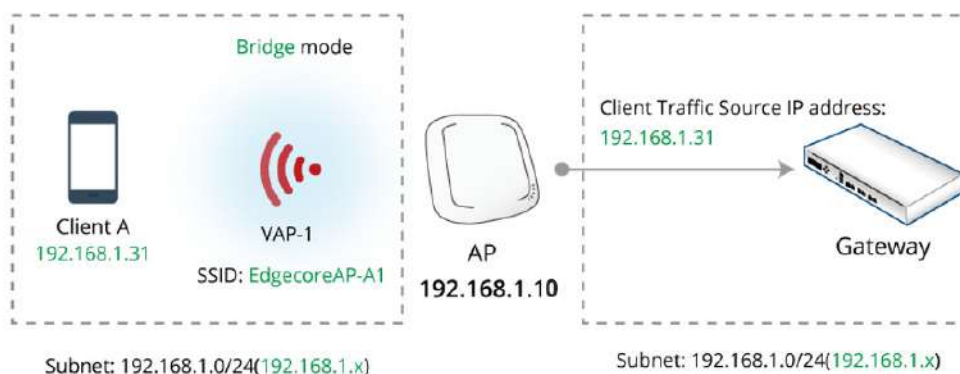
The screenshot shows the VAP Configuration page with the following settings:

- Profile Name:** RF Card A : VAP-1
- VAP:** ☒ Enable
- Profile Name:** VAP-1
- ESSID:** Guest Network
- Network Mode:** Bridge
- VLAN ID:** ☒ Disable
- CAPWAP Tunnel Interface:** Disable
- VAP:** ☒ Enable
- Profile Name:** VAP-1
- ESSID:** Guest Network
- Network Mode:** NAT
- DHCP Profile:** Pool 1
- DHCP Server:**
 - IP Address: 10.101.0.254
 - Netmask: 255.255.0.0
 - Start IP Address: 10.101.0.20
 - End IP Address: 10.101.0.100
 - Primary DNS Server: 8.8.8.8
 - Alternate DNS Server:
 - Domain Name:
 - Lease time: 1 Day
- CAPWAP Tunnel Interface:** Disable

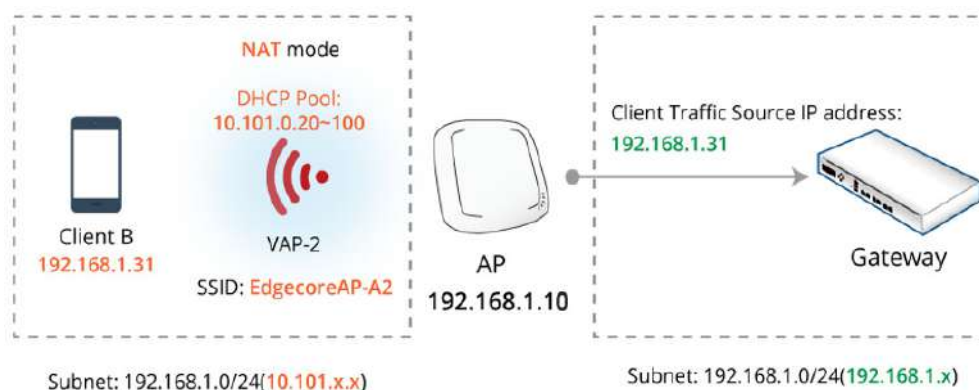
Select the specific VAP profile (in this case, “RF Card A : VAP-1”). The basic settings of the VAP are collected in the profile as follows:

- **VAP:** Disable or Enable this VAP.
- **Profile Name:** Name of the VAP profile for identity / management purposes.
- **ESSID:** Extended Service Set Identifier (ESSID) serves as an identifier for clients to associate with the specific VAP.
- **Network Mode:**
 - **Bridge** mode – the VAP operates transparently (i.e. no NAT, no DHCP) such that client devices will be assigned a dynamic IP address from a DHCP server on the LAN side. The source IP address of client traffic seen by the uplink gateway/switch will remain the

original IP address of the client (in this case, 192.168.1.31, as shown in the diagram below).



- **NAT mode** – the VAP operates like a Network Address Translation (NAT) device with a built-in DHCP server on this SSID such that client devices will be assigned a dynamic IP address from the configured DHCP pool on this SSID. After NAT conversion, the source IP address of client traffic seen by the uplink gateway/switch will be the IP address of the AP (in this case, 192.168.1.10, as shown in the diagram below).



- **VLAN ID:** Per-SSID VLAN tagging function – when enabled, clients' traffic which enters the AP through this SSID will be tagged with the configured VLAN ID.
- **DHCP Profile:** Built-in DHCP Server profile; IP settings of DHCP Server are under Home > System > DHCP Server.
- **CAPWAP Tunnel Interface:** Three states indicating the connectivity between AP and Controller, when AP is managed by Controller –
 - **Disable** (No Tunnel): the AP is operating with no CAPWAP Tunnel connection to the Controller
 - **Split Tunnel:** the AP passes only “control” traffic to the Controller via the CAPWAP Tunnel; i.e. “data” traffic will go out locally without passing through the Tunnel
 - **Complete Tunnel:** the AP passes both “control” and “data” traffic to the Controller via the CAPWAP Tunnel

- VLAN ID is supported only when the VAP is in Bridge mode.
- DHCP Profile and DHCP Server are activated only when the VAP is set to NAT mode.

►► Note:

- If the VAP is in NAT mode, the CAPWAP Tunnel Interface will only work in two states:
Disable (No Tunnel) or Split Tunnel.

Step 3: Configure General Wireless Settings

Under Home > Wireless > General, there are global settings for RF Card A and B. RF Card A is operating in 2.4 GHz band and RF Card B is operating in 5 GHz band, both of which are enabled by default.

For initial configuration, you might want to change the default basic settings shown below:

RF Card A – 2.4 GHz, 802.11g+802.11n, Antenna Mode 2T2R, Channel Width 40 MHz, Channel 6

RF Card B – 5 GHz, 802.11ac, Antenna Mode 2T2R, Channel Width 80 MHz, Channel 36

You can make changes to other settings at a later time.

The screenshot displays the 'General Settings' page for the wireless access point. The page is divided into two sections for RF Card A and RF Card B. RF Card A is configured for 2.4GHz, 802.11g+802.11n, 2T2R antenna mode, 20 MHz channel width, and channel 6. RF Card B is configured for 5GHz, 802.11ac, 2T2R antenna mode, 80 MHz channel width, and channel 36. Both cards have 'Short Preamble' and 'Short Guard Interval' set to 'Enable'.

Setting	RF Card A	RF Card B
RF Card Name	RF Card A	RF Card B
Band	2.4GHz	5GHz
Protocol	802.11g+802.11n	802.11ac
Short Preamble	Enable	Enable
Short Guard Interval	Enable	Enable
Antenna Mode	2T2R	2T2R
Channel Width	20 MHz	80 MHz
Channel	6	36
Transmit Power	Level 4	Level 4

Congratulations! After a system restart, the AP should be able to operate with these settings.

►► Note:

- SSID, ESSID, and BSSID:
- Service Set Identifier (SSID) is a key identifying the Name of a Wireless LAN.

- Extended Service Set Identifier (**ESSID**) = SSID; multiple physical APs can be configured to use the same SSID such that roaming across multiple physical APs is supported.
 - Basic Service Set Identifier (**BSSID**) = MAC address of AP; unique BSSID will be transmitted (in the Beacon management frame) when multiple physical APs broadcast the same ESSID.
-

2. Navigating the Web Management Interface

The APs have a web-based interface for configuration and management. This chapter will guide users through the AP's detailed settings. The following table shows all the function tabs under the **Main Menu** of Web Management Interface (WMI) of the AP.

System	Wireless	Firewall	Utilities	Status
General	VAP Overview	Firewall List	Change Password	Overview
Network Interface	General	Service	Backup & Restore	Interfaces
DHCP Server	VAP Config	Advanced	System Upgrade	Associated Clients
Management	Security		Reboot	DHCP Lease
CAPWAP	Repeater		Upload Certificate	Link Status
IPv6	Advanced		Background Scan	Event Log
iBeacon	Access Control		Discovery Utility	Wireless Log
RTLS	Hotspot 2.0		Network Utilities	Monitor
DPI DNS				

►► Note:

On each configuration page, you may click **SAVE** to save the changes of your configured settings, but you must reboot the system for the changes to take effect. After clicking **SAVE**, the following message will appear: **"Some modification has been saved and will take effect after Reboot."** All online users will be disconnected during reboot or restart.

3. System

Upon clicking the **System** icon, administrators can utilize this section for general configurations of the AP.

3.1 General

Home > System > System Information

System Information

Name : ECW5410-L *

Description :

Location :

Time

Device Time : 2000/01/02 23:50:05

Time Zone : (GMT+08:00)Taipei ▼

Time : ☒ Enable NTP ☐ Manually set up

NTP Server 1 : 192.168.1.254 *

NTP Server 2 : time.nist.gov

System Information

Name: The system name used to identify this system.

Description: Further information about the system (e.g. device model, firmware version, and active date).

Location: The information on geographical location of the system for the administrator to locate the system easily.

Time

Device Time: Display the current system time.

Time Zone: Select an appropriate time zone from the drop-down list box.

Time: There are two methods of setting up the time –

- **Enable NTP:** Synchronize the system clock with Network Time Protocol (NTP) server. Simply enter the IP Address or domain name of a local NTP server (if available, or search online for a NTP server nearest to you) and click **SAVE**.

Time Zone : (GMT+08:00)Taipei ▼

Time : ☒ Enable NTP ☐ Manually set up

NTP Server 1 : time.nist.gov *

NTP Server 2 :

- **Manually set up:** Set the system clock manually. This is the default method and requires setup every time when the system starts up. Simply choose a time zone, enter the date and the time accordingly, and click *SAVE*.

Time Zone : (GMT+08:00)Taipei ▼

Time : ☐ Enable NTP ☒ Manually set up

Set Date : 2017 ▼ Year 12 ▼ Month 18 ▼ Day

Set Time : 15 ▼ Hour 10 ▼ Min 00 ▼ Sec

Click **APPLY** after an alert message “*Some modifications have been saved and will take effect after **APPLY**.” appears on the WMI.



Unless Internet connection or NTP becomes unavailable, it is recommended to use NTP server for time synchronization because the system time needs to be reconfigured upon reboot.

3.2 Network Interface

On this page, the network settings of the device can be configured; fields with a red asterisk (i.e. **IP Address**, **Netmask**, **Default Gateway**, and **Primary DNS Server**) are mandatory.

General Network Interface DHCP Server Management CAPWAP IPv6 iBeacon RTLS DPI DNS

Home > System > Network Settings

Network Settings

Mode : ☒ Static ☐ DHCP

IP Address : 192.168.1.1 *

Netmask : 255.255.255.0 *

Default Gateway : 192.168.1.254 *

Primary DNS Server : 192.168.1.254 *

Alternate DNS Server :

Ethernet IGMP Snooping : ☒ Disable ☐ Enable

Layer2 STP :

Mode – Static: The administrator can manually set up the static LAN IP address. All required fields are marked with a red asterisk.

- **IP Address:** The IP address of the LAN port.
- **Netmask:** The Subnet mask of the LAN port.
- **Default Gateway:** The Gateway IP address of the LAN port.
- **Primary DNS Server:** The IP address of the primary DNS (Domain Name System) server.
- **Alternate DNS Server:** The IP address of the substitute DNS server.

Mode – DHCP: This configuration type is applicable when the system is connected to a network with the presence of a DHCP server; all related IP information required will be provided by the DHCP server automatically.

Ethernet IGMP Snooping: When Enabled, the switch forwards traffic IGMP packets are transferred via the Access Point's network interface and the IP multicast host. Registration information is recorded and sorted into multicast groups. The internal switch forwards traffic only to those ports that request multicast traffic. Adversely, without IGMP snooping, multicast traffic is treated like broadcast traffic, with packets forwarded to all ports causing network inefficiencies.

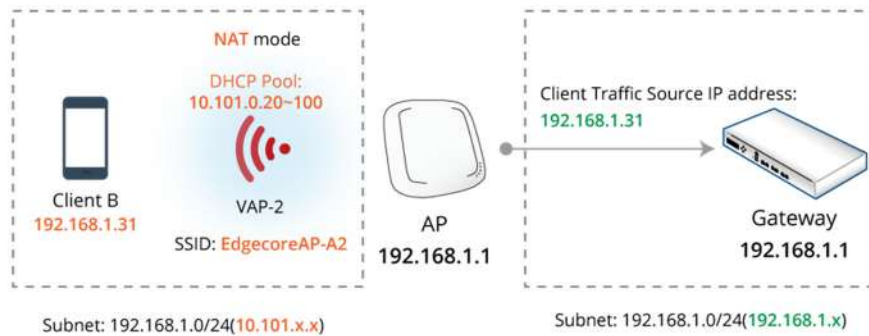
Layer 2 STP: If the AP is set up to bridge other network components, this option can be enabled to prevent undesired loops because a broadcasting storm may occur in a multi-switch environment where broadcast packets are forwarded in an endless loop between switches. Moreover, a broadcast storm may

consume most of the available system resources in addition to available bandwidth. Thus, enabling the Layer 2 STP can lower such undesired occurrence and derive the best available data path for network communication. The AP also supports RSTP Operation. Configurable parameters include **Bridge Priority**, **Hello Time**, **Max Age**, and **Forward Delay**. Please refer to IEEE standards for recommended parameter values.

Layer2 STP :	<div>RSTP (STP Compatibility) ▼</div>
	Bridge Priority : <div>32768 ▼</div>
	Hello Time : <div>2</div> * (1 - 10 seconds)
	Max Age : <div>20</div> * (6 - 40 seconds)
	Forward Delay : <div>15</div> * (4 - 30 seconds)

3.3 DHCP Server

When one VAP is enabled to operate in NAT mode, associated client devices will be assigned a dynamic DHCP IP address from the configured DHCP pool on the SSID. The NAT and DHCP mode can be executed without tunnel or managed by Edgecore WLAN controller with split tunnel.



It is noted that Pool1 – Pool16 are all configured as A class DHCP IP addresses as default values, and only configurable at AP's Web Management Interface. It starts from 10.101.0.254/16 to 10.116.0.254/16 for 16 DHCP Profiles, and DHCP lease time is 1440 minutes in default.

General Network Interface DHCP Server Management CAPWAP IPv6 iBeacon RTLS DPI DNS

Home > System > DHCP Server

DHCP Server Configuration

DHCP Profile : Pool 1

DHCP Server :

IP Address : 10.101.0.254 *

Netmask : 255.255.0.0 *

Start IP Address : 10.101.0.20 *

End IP Address : 10.101.0.100 *

Primary DNS Server : 8.8.8.8 *

Alternate DNS Server :

Domain Name :

Lease time : 1 Day

3.4 Management

The screenshot shows the 'Management Services' configuration page. At the top, there are tabs for 'General', 'Network Interface', 'DHCP Server', 'Management', 'CAPWAP', 'IPv6', 'iBeacon', 'RTLS', and 'DPI DNS'. The 'Management' tab is selected. Below the tabs, the breadcrumb 'Home > System > Management Services' is visible. The main title is 'Management Services'. On the left, there are labels for 'VLAN for Management:', 'SNMP Configuration:', 'Syslog Level:', 'Remote Syslog Server:', 'Management IP List:', and 'LED:'. The right side contains the configuration options: 'VLAN for Management' with 'Disable' (selected) and 'Enable' radio buttons, a 'VLAN ID' field with a red error message '* (1 - 4094)', 'SNMP Configuration' with 'Disable' and 'Enable' (selected) radio buttons, 'Community String' with 'Read' (public) and 'Write' (private) fields, an 'Edit SNMPv3 User List' button, 'Trap' with 'Disable' (selected) and 'Enable' radio buttons, a 'Server IP' field, 'Syslog Level' with a dropdown menu set to 'Debug', 'Remote Syslog Server' with 'Disable' (selected) and 'Enable' radio buttons, 'Server IP' and 'Server Port' (514) fields, 'Management IP List' with an 'Edit Management IP List' button, and 'LED' with 'Disable' and 'Enable' (selected) radio buttons.

VLAN for Management: When this is enabled, management traffic from the system will be tagged with a VLAN ID. In other words, administrators who need to access the WMI must send management traffic with the same VLAN ID such as connecting to a specific VAP with the same VLAN ID. Enter a value between 1 and 4094 for the VLAN ID if the option is enabled.

SNMP Configuration: to obtain the system information remotely.

- **Enable/ Disable:** *Enable* or *Disable* this function.
- **Community String:** The community string is required when accessing the Management Information Base (MIB) of the system. **Read:** Enter the community string to access the MIB with Read privilege. **Write:** Enter the community string to access the MIB with Write privilege.
- **Edit SNMPv3 User List:** The system allows 5 SNMP Users with Read or Read & Write Access. Determine the Name and Authentication Password on the SNMP Account List.
- **Trap:** When enabled, events on Cold Start, Interface UP & Down, and Association & Disassociation can be reported to the assigned server.
- **Server IP Address:** Enter the IP address of the assigned server that will receive the trap report.

Syslog Level: Select the desired level of received events from the drop-down menu. "Debug" level is as default setting.

Remote Syslog Server: When this function is enabled, specify an external SYSLOG server to receive SYSLOG messages from the system remotely.

- **Enable/ Disable:** *Enable* or *Disable* this function.
- **SYSLOG Server IP:** The IP address of the Syslog server that will receive the reported events.
- **Server Port:** The port number of the Syslog server.

Management IP List: Enter source IP address/subnet of administrator PCs which are allowed to access the WMI of this AP. Anyone else that is not on this List will be denied for WMI access. The default entry 0.0.0.0/0.0.0.0 means that administrators are allowed to access the WMI from anywhere.

LED: To turn on or off the Status LED indicator on the AP.

3.5 CAPWAP

CAPWAP is a standard interoperable protocol that enables a controller to manage a collection of wireless access points. There are 5 methods of auto AP discovery, namely DNS SRV, DHCP option, Broadcast, Multicast, and Static.

Home > System > CAPWAP Configuration

CAPWAP Configuration

CAPWAP : ☒ Disable ☐ Enable

Certificate Date Check : ☐ Disable ☐ Enable [Manage Certificates](#)

DNS SRV Discovery : ☐ Disable ☒ Enable
Domain Name Suffix :

DHCP Option Discovery : ☐ Disable ☒ Enable

Broadcast Discovery : ☐ Disable ☒ Enable

Multicast Discovery : ☐ Disable ☒ Enable

Static Discovery : ☐ Disable ☒ Enable

Pri.	AC Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>

CAPWAP: Enable or Disable the CAPWAP feature.

Certificate Date Check: To enable this item, select *Enable* and click *Manage Certificates* to enter the Upload Certificate page. Please refer to the section 6.5 Upload Certificate.

DNS SRV Discovery: Using DNS SRV to discover access controller.

- **Domain Name Suffix:** Enter the suffix of the access controller, such as example.com.

DHCP Option Discovery: Using DHCP option to discover access controller.

Broadcast Discovery: Using Broadcast to discover access controller.

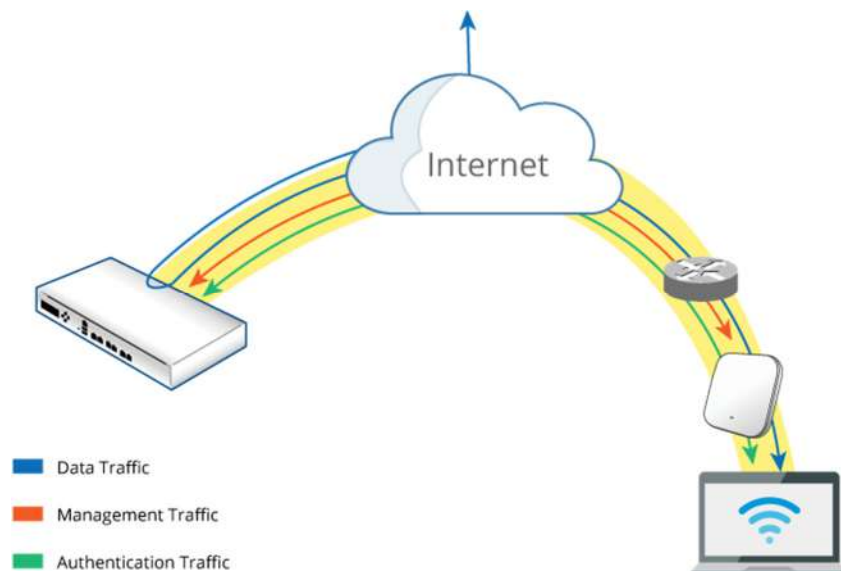
Multicast Discovery: Using muticast to discover access controller.

Static Discovery: Using Static approach to discover access controller.

- **AC Address:** The IP address of the access controller. If it can not discover the first AC, it will try to discover the second AC.

3.5.1 To Manage by WLAN Controller with Complete Tunnel

Complete Tunnel uses the CAPWAP protocol to communicate with an Access Point so that all management traffic, authentication traffic and data traffic from the service area AP provided are transmitted back to the Controller, before forwarding data traffic to the internet. The WLAN controller is able to implement role-based policies over Layer 3 networks, with user access control available in the remote sites. This feature allows the WLAN controller to fully support centralized AP management and user management.



The following procedures may be helpful

1. On AP: to type the IP address for **Static Discovery** and wait until the CAPWAP column displays a “RUN” status.
2. On WHG: to prepare Template of the **VAP configuration** with **CAPWAP Tunnel Interface** – “**Complete Tunnel**”
3. On WHG: to apply the prepared Template to the CAPWAP-establish AP and the Tunnel status will show a clickable “Edit” button in black if a VAP is configured to be tunneled back to the controller

Add

Delete

Add to Map / Floor Plan

Backup Config

Restore Config

Upgrade

Apply Settings

Reboot

	Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.
<input type="checkbox"/>	ECW5211-L	ECW5211-L	10.73.7.38	00:1F:D4:06:F1:1D	Overview	2	Online	0	<div>Edit</div>	<div>System Overview</div> <div>Go</div>	RUN	3.43.00

4. On AP: to check the AP WMI showing Data Channel is “Active” with the VAP tunnel status in “Green” light on the System Overview page

LAN Interface

MAC Address	00:1F:D4:06:F1:1D
IP Address	10.73.7.38
Subnet Mask	255.255.0.0
Gateway	10.73.1.254

AP Status

RF Card Name : RF Card A ▼

Profile Name	BSSID	ESSID	Security Type	Online Clients	TUN
VAP-1	00:1F:D4:06:F1:1F	Guest Network	Open	0	✔

CAPWAP

Status	Run(10.71.1.81)
Data Channel	Active

IPv6

Status Disabled

5. On AP: to reconfirm the specific VAP Configuration is under **Complete Tunnel**

System

Wireless

Firewall

Utilities

Status

VAP Overview

General

VAP Config

Security

Repeater

Advanced

Access Control

Hotspot 2.0

Home > Wireless > VAP Configuration

VAP Configuration

VAP : ☐ Disable ☒ Enable

Profile Name : VAP-1

ESSID : Guest Network

Network Mode : Bridge ▼

Uplink Bandwidth : 0 Kbits/s *(1-1048576, 0:Disable)

Downlink Bandwidth : 0 Kbits/s *(1-1048576, 0:Disable)

VLAN ID : ☐ Disable ☒ Enable

VLAN ID : 1000 *(1 - 4094)

Uplink 802.1p : Best Effort (BE) ▼

CAPWAP Tunnel Interface : Complete Tunnel ▼

Service Zone : SZ0 ▼

Profile Name : RF Card A : VAP-1 ▼

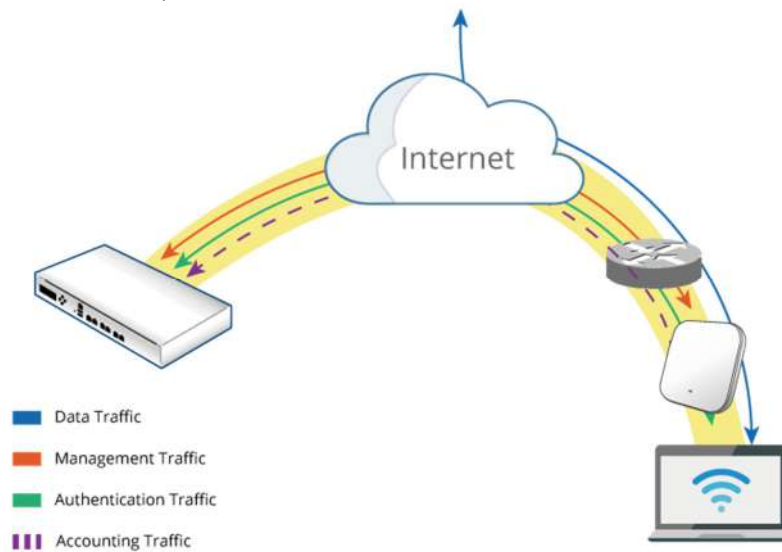
SAVE

CLEAR

6.

3.5.2 To Manage by WLAN Controller with Split Tunnel

For **Split Tunnel**, only user authentication related traffic will be directed back to the controller. For authenticated users, data traffic will go to the Internet through the local network directly. The user data can be transmitted with a shorter path and the network load of the controller can also be reduced.



The following procedures may be helpful

1. On AP: to type the IP address for **Static Discovery**, and wait until the CAPWAP column displays a “RUN” status.
2. On WHG: to prepare Template of the **VAP configuration** with **CAPWAP Tunnel Interface – “Split Tunnel”**
3. On WHG: to apply the prepared Template to the CAPWAP-establish AP and the Tunnel status will show a clickable “Edit” button in black if a VAP is configured to be tunneled back to the controller.

Add

Delete

Add to Map / Floor Plan


Backup Config

Restore Config

Upgrade

Apply Settings

Reboot

	Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.
	ECW5211-L	ECW5211-L	10.73.7.38	00:1F:D4:06:F1:1D	Overview	1	Online	0	<div>Edit</div>	<div>System Overview</div> <div>Go</div>	RUN	3.43.00

4. On AP: to check the AP WMI showing Data Channel is “Active” with the VAP tunnel status in “Green” light on the System Overview page

LAN Interface

MAC Address	00:1F:D4:06:F1:1D
IP Address	10.73.7.38
Subnet Mask	255.255.0.0
Gateway	10.73.1.254

AP Status

RF Card Name : RF Card A ▼

Profile Name	BSSID	ESSID	Security Type	Online Clients	TUN
VAP-1	00:1F:D4:06:F1:1F	Guest Network	Open	0	

CAPWAP

Status	Run(10.71.1.81)
Data Channel	Active

IPv6

Status Disabled

5. On AP: to reconfirm the specific VAP Configuration is under **Split Tunnel**

System

Wireless

Firewall

Utilities

Status

VAP OverviewGeneralVAP ConfigSecurityRepeaterAdvancedAccess ControlHotspot 2.0

Home > Wireless > VAP Configuration

VAP Configuration

Profile Name : RF Card A : VAP-1 ▼

VAP : ☐ Disable ☒ Enable

Profile Name : VAP-1

ESSID : Guest Network

Network Mode : Bridge ▼

Uplink Bandwidth : 10 Kbits/s *(1-1048576, 0:Disable)

Downlink Bandwidth : 10 Kbits/s *(1-1048576, 0:Disable)

VLAN ID : ☐ Disable ☒ Enable

VLAN ID : 12 *(1 - 4094)

Uplink 802.1p : Best Effort (BE) ▼

CAPWAP Tunnel Interface : Split Tunnel ▼

Service Zone : SZ0 ▼

SAVE

CLEAR

3.6 IPv6

IPv6 and IPv4 dual stack addressing capability is supported.

Status: IPv6 by default is disabled but it can be enabled on this tab page.

Mode: There are two options for acquiring an IPv6 address for this device.

- **Static:** Configuring IPv6 address manually via this option if you have already acquired a permanent IPv6 address for operation.
- **DHCP:** Acquire IPv6 address automatically from upstream server.

3.7 iBeacon (ECW5211-L, ECW5410-L, ECWO5211-L Only)

iBeacon is a technology, introduced by Apple in 2013, enabling new location awareness services. When properly configured, the AP becomes an iBeacon-compatible hardware transmitter which broadcasts information to nearby devices via Bluetooth Low Energy (BLE; a wireless connectivity technology).

The UUID, Major and Minor are the identifying parameters used to make up the key component of the iBeacon "Advertising Packets" that are continually transmitted by the AP.

- **UUID:** Universally Unique Identifier, a number to distinguish your own AP in the network, from all other iBeacon transmitters in networks outside your control. It contains 32 hexadecimal digits, split into 5 groups and should look something like this: 12345678-ABCD-EFAB-CDEF-1234567890AB

- **Major & Minor:** These are numbers (integer values between 0 and 65535) assigned to your own AP in order to identify the AP with greater accuracy than using UUID alone. Normally, Major value is intended to identify and distinguish a group, while Minor value is intended to identify and distinguish an individual. For example, if there are many iBeacon transmitters deployed with the same UUID in a shopping center, and they are located at different floors/stores. Then these transmitters can be identified and distinguished by different Major (e.g. 1 for 1st floor) and Minor (e.g. 2 for 2nd store) values.

3.8 RTLS (ECW5211-L, ECW5410-L, ECWO5211-L Only)

To implement a Wi-Fi based location solution, customers can enable this feature to integrate the AP with the dedicated Linkyfi (technology partner) server of Real Time Location System (RTLS), which is part of Linkyfi Location Engine - an advanced software solution for indoor location and real-time navigation in all types of venues.

The screenshot shows the 'Real Time Location Tracking System' configuration page. At the top, there is a breadcrumb trail: 'Home > System > Real Time Location Tracking System'. Below this, the title 'Real Time Location Tracking System' is centered. The configuration options are as follows:

- Status :** ☒ Disable ☐ Enable
- Advanced Tracking(Beta) :** ☒ Disable ☐ Enable
- Server IP :** [Text Input Field] *(IPv4)
- Server Port :** [Text Input Field] *(49152 - 65535)
- Report Period :** [Text Input Field] *(2 - 60 sec.)

3.9 DPI DNS (ECW5211-L, ECW5410-L, ECWO5211-L Only)

To perform WiFi marketing analytics, customers can enable this feature to integrate the AP with Linkyfi's DNS server, which is also part of Linkyfi Location Engine that analyzes DNS traffic via Deep Packet Inspection (DPI) technology.

The screenshot shows the 'DPI DNS' configuration page. At the top, there is a breadcrumb trail: 'Home > System > DPI DNS'. Below this, the title 'DPI DNS' is centered. The configuration options are as follows:

- Status :** ☒ Disable ☐ Enable
- Server IP :** [Text Input Field] *(IPv4)
- Server Port :** [Text Input Field] *(49152 - 65535)
- Report Period :** [Text Input Field] *(2 - 60 sec.)

4. Wireless

This section includes the following functions: **VAP Overview**, **General**, **VAP Configuration**, **Security**, **Repeater**, **Advanced**, **Access Control** and **Hotspot 2.0**. The Edgecore Access Point supports up to sixteen Virtual Access Points (VAPs) per RF card. Each VAP can have its own settings (e.g. ESSID, VLAN ID, security settings, etc.). With such VAP capabilities, different levels of service can be configured to meet network requirements.

4.1 VAP Overview

An overall status is collected on this page, including **ESSID**, **Network Mode**, **State**, **Security Type**, **MAC ACL**, and **Hotspot 2.0**, where the AP features 16 VAPs per radio with respective settings. In this table, please click on the hyperlinks to further configure each individual VAP.

Home > Wireless > VAP Overview

VAP Overview

RF Card A

VAP No.	ESSID	Network Mode	State	Security Type	MAC ACL	Hotspot 2.0
1	Guest Network	Bridge	Enabled	Open	Disabled	Disabled
2	Virtual Access Point 1	Bridge	Disabled	Open	Disabled	Disabled
3	Virtual Access Point 2	Bridge	Disabled	Open	Disabled	Disabled

Up to 16 VAPs

RF Card B

VAP No.	ESSID	Network Mode	State	Security Type	MAC ACL	Hotspot 2.0
1	Guest Network	Bridge	Enabled	Open	Disabled	Disabled
2	Virtual Access Point 1	Bridge	Disabled	Open	Disabled	Disabled
3	Virtual Access Point 2	Bridge	Disabled	Open	Disabled	Disabled

Up to 16 VAPs

State: The hyperlink showing *Enable* or *Disable* links to the **VAP Configuration** page.

VAP Overview General **VAP Config** Security Repeater Advanced Access Control Hotspot 2.0

Home > Wireless > VAP Configuration

VAP Configuration

Profile Name : RF Card A : VAP-1 ▼

VAP : ☐ Disable ☒ Enable

Profile Name : VAP-1

ESSID : Guest Network

VLAN ID : ☒ Disable ☐ Enable

VLAN ID : 1 (1 - 4094)

CAPWAP Tunnel Interface : ☐

or

VAP Overview General **VAP Config** Security Repeater Advanced Access Control Hotspot 2.0

Home > Wireless > VAP Configuration

VAP Configuration

Profile Name : RF Card A : VAP-1 ▼

VAP : ☐ Disable ☒ Enable

Profile Name : VAP-1

ESSID : Guest Network

Network Mode : Bridge ▼

VLAN ID : ☒ Disable ☐ Enable

VLAN ID : 1 (1 - 4094)

CAPWAP Tunnel Interface : Disable ▼

VAP – State Page

- **Security Type:** The hyperlink showing the security type links to the **Security Settings** Page.

VAP Overview General VAP Config **Security** Repeater Advanced Access Control Hotspot 2.0

Home > Wireless > Security Settings

Security Settings

Profile Name : RF Card A : VAP-1 ▼

Security Type : **Open**
WEP
802.1X
WPA-Personal
WPA-Enterprise

☐ 802.11r roaming

VAP – Security Type Page

- **MAC ACL:** The hyperlink showing **Allow** or **Disable** links to the **Access Control Settings** Page.

The screenshot shows the 'Access Control Settings' page. At the top, there are tabs for System, Wireless, Firewall, Utilities, and Status. Below these are sub-tabs for VAP Overview, General, VAP Config, Security, Repeater, Advanced, Access Control, and Hotspot 2.0. The breadcrumb trail is 'Home > Wireless > Access Control Settings'. The main title is 'Access Control Settings'. It features a 'Profile Name' dropdown set to 'RF Card A : VAP-1'. Below this, 'Maximum Number of Clients' is set to 128, with a note '(Range: 1 ~ 256 per RF card)'. 'Access Control Type' is set to 'Disable Access Control'.

[VAP – MAC ACL Page](#)

- **Hotspot 2.0:** The advanced settings hyperlink links to the **Hotspot 2.0** Page.

The screenshot shows the 'Hotspot 2.0' configuration page. It has the same top navigation and sub-tab structure as the previous page. The breadcrumb trail is 'Home > Wireless > Hotspot 2.0'. The main title is 'Hotspot 2.0'. It features a 'Profile Name' dropdown set to 'RF Card A : VAP-1'. Below this, there are radio buttons for 'Status' (Disable selected, Enable unselected) and 'Internet Access' (Disable selected, Enable unselected). 'Access Network Type' is set to 'Private network'. 'Venue Information' includes a 'Group' dropdown set to 'Unspecified' and a 'Type' dropdown set to 'Unspecified'. 'Venue Name List' contains five entries, each with a language dropdown (all set to 'English') and a text input field.

[VAP – Hotspot 2.0 Page](#)

4.2 General

The screenshot shows the 'General Settings' page for the wireless interface. The 'RF Card Name' is set to 'RF Card A'. The 'Band' is set to '2.4GHz'. The 'Protocol' is set to '802.11g+802.11n'. The 'Short Preamble' is set to 'Enable'. The 'Short Guard Interval' is set to 'Enable'. The 'Antenna Mode' is set to '2T2R'. The 'Channel Width' is set to '20 MHz'. The 'Channel' is set to '6'. The 'Transmit Power' is set to 'Level 1'. The 'Beacon Interval' is set to '100' milliseconds. The 'Airtime Fairness' is set to 'Disable'. The 'Packet Delay Threshold' is set to '0' milliseconds. The 'Idle Timeout' is set to '300' seconds. The 'Band Steering' is set to 'Disable'. The 'Interference Detection' is set to 'Utilization Threshold 0%'. The 'WME Configuration' is set to 'Configure'. The 'Transmission Rate Threshold' is set to '1001' kbps. The 'U-APSD' is set to 'Enable'.

AP's system general wireless settings can be configured

RF Card Name: Select one RF card for further configuration.

Band: Select **Disable** if the wireless function is not required.

Protocol: Select an appropriate wireless protocol: *802.11a*, *802.11a+802.11n*, *802.11ac* or *802.11b*, *802.11g*, *802.11b+802.11g*, *802.11g+802.11n*. The protocol is dependent on the Band of the RF Card.

- **Pure 11n:** Enable 802.11n network only.

Short Preamble: The short preamble with a 56-bit synchronization field can improve WLAN transmission efficiency. Select **Enable** to use Short Preamble or **Disable** to use Long Preamble with a 128-bit synchronization field.

Short Guard Interval (available when Band is 802.11g+802.11n or 802.11a+802.11n): The guard interval is the space between symbols (characters) being transmitted to eliminate inter-symbol interference. In order to further boost throughput with **802.11n**, short guard interval is half of what it used to be; please select **Enable** to use Short Guard Interval or **Disable** to use normal Guard Interval.

Antenna Mode (ECW5211-L, ECW5410-L, ECW05210-L, ECW05211-L only): Select 1T1R for one spatial stream or 2T2R for two spatial streams.

Channel Width: Double channel bandwidth to 40 MHz or 80 MHz to enhance throughput.

Channel: Select the appropriate channel from the drop-down menu to meet the regularity.

- When configured as "Auto" in Radio Card B, there is channel selector table for channel switching when the chosen channel is interfered or DFS channel signal is detected

- For outdoor AP models, the “Outdoor mode” will affect the channel selection

Max Transmit Rate (ECW5210-L only): The maximum wireless transmit rate can be selected from the drop-down menu. The system will use the highest possible rate when Auto is selected. Please note that MCS0 ~ MCS23 are transmit rates only for n bands.

Transmit Power: The signal strength transmitted from the system can be selected by Levels.

- Each Level signifies a decrement of 1dBm from the highest power.
- Level 1 is the actual highest power, while Level 2 is the highest power minus 1dBm, so on and so forth.

ACK Timeout: It indicates a period of time when the system waits for an AcknECWOedgement frame sent back from a station without retransmission. In other words, upon timeout, if the AcknECWOedgement frame is still not received, the frames will be retransmitted. This option can be used to tune network performance for extended coverage. For regular indoor deployments, please keep the default setting.

Beacon Interval (ms): The entered amount of time indicates how often the beacon signal will be sent from the access point.

- The Beacon Interval must be greater than 500ms when more than 7 VAPs are enabled.
- The Beacon Interval must be greater than 250ms when more than 3 VAPs are enabled

Airtime Fairness: when 802.11a/b/g/n legacy devices occupy airtime, throughput for 802.11ac devices is affected.

- Enable: to ensure all devices with different band compatibilities have the same air time. This feature is ideal for networks with devices supporting different bands.
- Preferred Access: N band clients are prioritized. This feature is ideal for networks with devices supporting different bands.

Packet Delay Threshold (ms): An Access Point may be occupied trying to transmit a packet to a busy client or a client out of range, hence delaying transmission to other connected clients. When Enabled, this Tx queue flushing mechanism drops packets and immediately begins to process others if the queue has been processed for more than x milliseconds, where Default = 0 (disabled). This feature improves the performance of complex wireless networks but may require some packets to be resent.

Idle Timeout (s): Client disconnects when inactivity reaches the configured amount of time in seconds, where default = 300s.

Band Steering: When enabled, clients with 5GHz connectivity will be steered towards the 5GHz band to reduce congestion in the 2.4GHz band. This is applicable only when the AP is set to 2.4GHz and 5GHz on the 2 RF Cards.

- Aggressive: clients with 5GHz connectivity are forced to connect to the 5GHz band.

- Note that this is a general setting for the Access Point, and is not set per RF Card.

Interference Detection: When Utilization, Latency (and Invalid Packet Rate) of the current channel or adjacent channel reaches the configured threshold (in %), the AP switches to a different Channel.

WME Configuration: Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. Access priority can be configured using with different parameters. CW Min: Contention Window Minimum, CW Max: Contention Window Maximum, AIFS: Arbitration Inter Frame Spacing, TXOP Limit: Transmission Opportunity Limit.

Transmission Rate Threshold: The client will be kicked when transmission rate is lower than the configured threshold. This ensures high connection speed for all associated clients.

U-APSD: U-APSD stands for **U**nscheduled **A**utomatic **P**ower **S**ave **D**elivery, an 802.11 power save mechanism that works with WMM. When a client device is in Power Save mode (i.e. its receiver is turned off and thus cannot receive any data frames), the AP will temporarily buffer all frames destined to the client.

►► Note: Features such as Short Preamble, ACK Timeout, and may be limited on RF Card B.

Table 1 RF Configurations (under normal circumstances in certain countries)

Band	Channel	Rate	Power
Disable	N/A	N/A	N/A
802.11a	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165	6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M	Auto
802.11b	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	1M, 2M, 5.5M, 11M	
802.11g	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M	
802.11b+802.11g	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	1M, 2M, 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M	
802.11a+802.11n	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165	6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M, MCS0~23	Level 1 ~ Level 25 (model dependent)
802.11n+802.11g	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	1M, 2M, 5.5M, 11M, 12M, 18M, 24M, 36M, 48M, 54M, MCS0~23	
802.11ac	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165	MCS7-9	

*Please note that available values above will vary depending on the regulation of different countries.

4.3 VAP Config

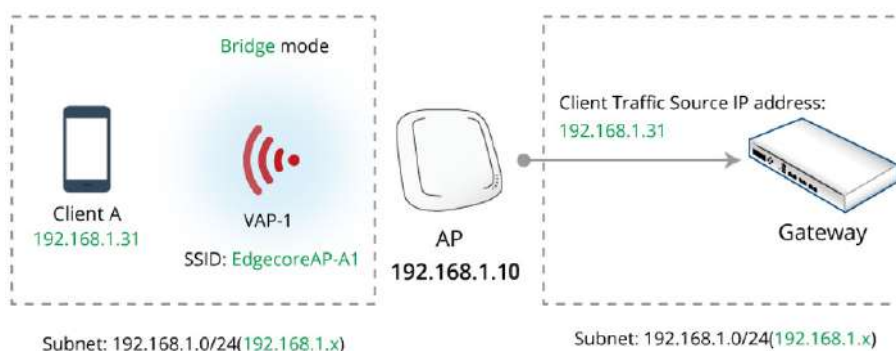
This section provides configuration of each Virtual Access Point with settings such as **Profile Name**, **ESSID**, and **VLAN ID**. To enable specific VAP, select the VAP from the drop-down list of Profile Name.

VAP: Disable or Enable this VAP.

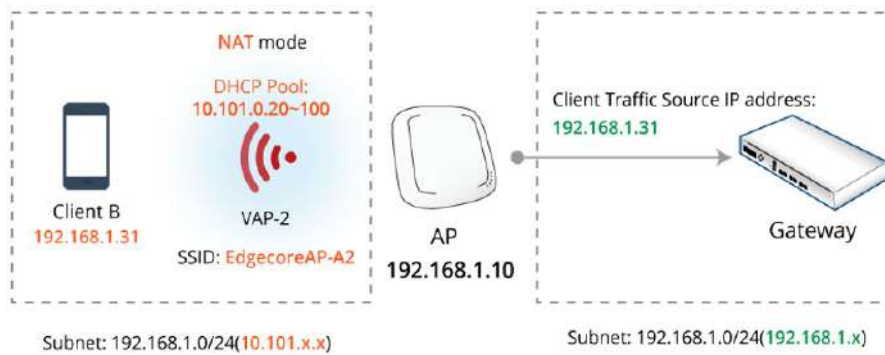
Profile Name: Name of the VAP profile for identity / management purposes.

ESSID: Extended Service Set Identifier (ESSID) serves as an identifier for clients to associate with the specific VAP.

Network Mode – Bridge mode: the VAP operates transparently (i.e. no NAT, no DHCP) such that client devices will be assigned a dynamic IP address from a DHCP server on the LAN side. The source IP address of client traffic seen by the uplink gateway/switch will remain the original IP address of the client (in this case, 192.168.1.31, as shown in the diagram below).



Network Mode – NAT mode (ECW5211-L, ECW5410-L, ECWO5211-L only): the VAP operates like a Network Address Translation (NAT) device with a built-in DHCP server on this SSID such that client devices will be assigned a dynamic IP address from the configured DHCP pool on this SSID. After NAT conversion, the source IP address of client traffic seen by the uplink gateway/switch will be the IP address of the AP (in this case, 192.168.1.10, as shown in the diagram below).



Uplink/Downlink Bandwidth: Bandwidth control is configurable on the VAP in Kbits per second. Set 0 for unlimited bandwidth control.

VLAN ID: Per-SSID VLAN tagging function – when enabled, clients’ traffic which enters the AP through this SSID will be tagged with the configured VLAN ID.

Uplink 802.1P per VAP: Priority levels for uplink traffic can be selected here. The options available are Background, Best Effort, Excellent Effort, Critical Applications, Video, Voice, Internetwork Control, Network Control. For more information, please refer to IEEE Standards 802.1P.

DHCP Profile (for NAT mode): Built-in DHCP Server profile; IP settings of DHCP Server are under Home > System > DHCP Server.

CAPWAP Tunnel Interface: Three states indicating the connectivity between AP and Controller, when AP is managed by Controller

- **Disable (No Tunnel):** the AP is operating with no CAPWAP Tunnel connection to the Controller
- **Split Tunnel:** the AP passes only “control” traffic to the Controller via the CAPWAP Tunnel; i.e. “data” traffic will go out locally without passing through the Tunnel
- **Complete Tunnel:** the AP passes both “control” and “data” traffic to the Controller via the CAPWAP Tunnel

►► Note:

-
- VLAN ID is supported only when the VAP is in Bridge mode.
 - DHCP Profile and DHCP Server are activated only when the VAP is set to NAT mode.
 - If the VAP is in NAT mode, the CAPWAP Tunnel Interface will only work in two states: Disable (No Tunnel) or Split Tunnel.
-

4.4 Security

The AP supports various wireless authentication and data encryption methods in each VAP profile. With this, the administrator can provide different service levels to clients. The security type includes **Open**, **WEP**, **WPA-Personal**, **WPA-Enterprise**, and **OSEN**.



Open: Authentication is not required and data is not encrypted during transmission.

WEP: Wired Equivalent Privacy is a data encryption mechanism based on a 64-bit, 128-bit, or 152-bit shared key algorithm.



- **802.11 Authentication:** Select from *Open System*, *Shared Key*, or *Auto*.
- **WEP Key Length:** Select a key length from *64-bit*, *128-bit*, or *152-bit*.
- **WEP Key Format:** Select a WEP key format from *ASCII* or *Hex*.
- **WEP Key Index:** Select a key index from **1~4**. The WEP key index is a number that specifies which WEP key will be used for the encryption of wireless frames during data transmission.
- **WEP Keys:** Provide the pre-defined WEP key value; the system supports up to 4 sets of WEP keys.

► Note: 152 bits WEP key length may be limited on selected AP models.

WPA-Personal: WPA-Personal is a Pre-Shared Key (PSK) authentication method.

- **802.11r Roaming:** Roaming is possible for clients within the same Mobility Domain on different APs with the same Encryption Key.

Security Settings

Profile Name : RF Card A : VAP-1 ▼

Security Type : WPA-Personal ▼ ☒ 802.11r roaming

Cipher Suite : WPA2 ▼

Protected Management Frames : Optional ▼

Roaming Target AP List :

Pre-shared Key Type : ☐ PSK(Hex)*(64 chars) ☒ Passphrase*(8 - 63 chars)

Pre-shared Key :

Group Key Update Period : 86400 second(s)

- **Cipher Suite:** Select an encryption method from **WPA2** or **WPA2/WPA**.
- **Protected Management Frames:** Select Disable, Optional or Mandatory.
- **Roaming Target AP List** (when 802.11r is enabled)

802.11r Roaming Settings

Profile Name : RF Card A : VAP-1 ▼

Mobility Domain :

VAP MAC Address : 00:1F:D4:AC:5E:9C

Encryption Key :

Transition Over the DS : ☒ Disable ☐ Enable

No	Target VAP MAC Address	Encryption Key
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>

- **Pre-shared Key Type:** Select a pre-shared key type: PSK (Hex) or Passphrase.
- **Pre-shared Key:** Enter the key value for the pre-shared key; the format of the key value depends on the key type selected.
- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in seconds.

WPA-Enterprise: When selected, the RADIUS authentication and data encryption will both be enabled.

Security Settings

Profile Name : RF Card A : VAP-1

Security Type : WPA-Enterprise ☒ 802.11r roaming

Cipher Suite : WPA2

Protected Management Frames : Optional

Roaming Target AP List : [Configure](#)

Group Key Update Period : 86400 second(s)

Primary RADIUS Server :

Host : *(Domain Name / IP Address)

Authentication Port : 1812 *

Secret Key : **

Accounting Service : ☒ Disable ☐ Enable

Accounting Port : 1813 *

Accounting Interim Update Interval : 60 second(s) *

Secondary RADIUS Server :

Host : (Domain Name / IP Address)

Authentication Port :

Secret Key :

Accounting Service : ☒ Disable ☐ Enable

Accounting Port :

Accounting Interim Update Interval : second(s)

Security Settings: WPA-Enterprise

- **Cipher Suite:** Select an encryption method from **WPA2** or **WPA2/WPA**.
- **Protected Management Frames:** Select Disable, Optional or Mandatory.
- **Roaming Target AP List** (when 802.11r is enabled)

802.11r Roaming Settings

Profile Name : RF Card A : VAP-1

Mobility Domain :

VAP MAC Address : 00:1F:D4:AC:5E:9C

Encryption Key :

Transition Over the DS : ☒ Disable ☐ Enable

No	Target VAP MAC Address	Encryption Key
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>

- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in seconds.
- **RADIUS Server Settings (Primary/Secondary):**
 - o **Host:** Enter the IP address or domain name of the RADIUS server.
 - o **Authentication Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1812.
 - o **Secret Key:** The secret key for the system to communicate with the RADIUS server.

- **Accounting Service:** *Enabling* this option allows accounting of login and logouts through the RADIUS server.
- **Accounting Port:** The port number used by the RADIUS server for accounting purposes. Specify a port number or use the default, 1813.
- **Accounting Interim Update Interval:** The system will update accounting information to the RADIUS server every interval period.

OSEN: OSEN stands for “The Online Signup (OSU) Server-only authenticated layer 2 Encryption Network, which is “Hotspot 2.0 Release2” (HS2.0 R2) authentication method. Before setting HS2.0 R2, we should check the security of each VAP, HS2.0 VAP (VAP1: WPA-Enterprise) or OSEN VAP (VAP2: OSEN). Further configuration detail; please check “*session 4.8 Hotspot 2.0.*”

4.5 Repeater

The AP is capable of utilizing WDS to extend wireless network coverage. It supports up to 8 WDS links to its peer APs per radio. Fill in remote peer's MAC address and click **SAVE** to proceed.

VAP Overview General VAP Config Security Repeater Advanced Access Control Hotspot 2.0

Home > Wireless > Repeater Settings

Repeater Settings

Repeater Type : WDS ▼

WDS Profile : RF Card A : WDS Link 1 ▼

WDS : Enable ▼

WDS Link Address : 0A:1F:D4:A0:C6:BA **Please use it as the peer's Remote AP MAC Address*

Remote AP MAC Address :

Security Type : None ▼

CAPWAP Tunnel Interface : ☐

WDS: *Enable* or *Disable* the selected WDS Link profile.

WDS Link Address: The MAC address of the AP interface for the selected WDS Link.

Remote AP MAC Address: The MAC address of remote peer.

Security Type: None, WEP, or WPA-Personal.

CAPWAP Tunnel Interface: Check this option to designate WDS traffic to pass through CAPWAP Tunnel established between the AP and the controller.

4.6 Advanced

The administrator can adjust the following parameters to improve network communication performance if a poor connection occurs.

Home > Wireless > Advanced Wireless Settings

Advanced Wireless Settings

Profile Name : RF Card A : VAP-1

RTS Threshold : 2346 *(1 - 2346)

DTIM period : 1 *(1 - 15)

Consecutive Dropped Packets : 5 *(2 - 50, 0:Disable)

Broadcast SSID : ☐ Disable ☒ Enable

Wireless Station Isolation : ☐ Disable ☒ Enable

IAPP : ☐ Disable ☒ Enable

Multicast-to-Unicast Conversion : ☒ Disable ☐ Enable

TX STBC : ☐ Disable ☒ Enable

Multicast/Broadcast Rate : 5.5M

Management Frame Rate : 5.5M

Receiving RSSI Threshold : 0 dBm *(-95 ~ 0, 0:Disable)

RTS Threshold: Enter a value between 1 and 2346. RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the fragment to prevent the hidden node problem. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with the AP or in areas where the clients are far apart and can detect only the AP but not each other.

Fragmentation Threshold (802.11a, 802.11b and 802.11g Modes): Enter a value between 256 and 2346. A packet size larger than this threshold will be fragmented (sent with several pieces instead of one chunk) before transmission. A smaller value results in smaller frames but allows a larger number of frames in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.

DTIM Period: Input the DTIM Interval that is generated within the periodic beacon at a specified frequency. Higher DTIM will allow the wireless client to save more energy, but the throughput will be lowered.

Consecutive Dropped Packets: This is the maximum number of transmission retries the AP will attempt when packet transmission is dropped before deciding the client is out of transmission reach. When transmission retries fails for the set number of times, the Access Point kicks the client to optimize performance for other connected clients.

Broadcast SSID: Disabling this function will stop the system from broadcasting its SSID. If broadcast of the SSID is disabled, only devices that have the correct SSID can connect to the system.

Wireless Station Isolation: By enabling this function, all stations associated with the system are isolated and can only communicate with the system.

IAPP: IAPP (Inter Access Point Protocol) is a protocol by which access points share information about the stations connected to them. When this function is enabled, the system will automatically broadcast information of associated wireless stations to its peer access points. This will help wireless stations roam smoothly among IAPP-enabled access points in the same wireless LAN.

Multicast-to-Unicast Conversion: When Multicast-to-Unicast Conversion is enabled, the Access Point intelligently forwards traffic only to those ports that request multicast traffic. Adversely, when disabled, multicast traffic is treated like broadcast traffic, with packets forwarded to all ports causing network inefficiencies.

TX STBC: STBC is a pre-transmission encoding done by MIMO transmitter that allows it to improve the signal-to-noise ratio even at a single RF receiver (non-MIMO).

Multicast/Broadcast Rate: Bandwidth configuration for multicast/broadcast packets. If your wireless clients require a larger or smaller bandwidth for sending multicast/ broadcast packets, the administrator can customize the Access Point's multicast/ broadcast bandwidth here.

Management Frame Rate: This feature controls the bandwidth for Management Frames. The higher the rate it, the shorter range the transmission covers

Receiving RSSI Threshold: To ensure connected stations have quality connection speeds, a station will not be able to associate to the network unless its receiving sensitivity meets the configured threshold.

►► Note: TX STBC may be limited on selected AP models.

4.7 Access Control

On this page, the network administrator can restrict the total number of clients connected to the Access Point, as well as specify particular MAC addresses that can or cannot access the device.



System Wireless Firewall Utilities Status

VAP Overview General VAP Config Security Repeater Advanced Access Control Hotspot 2.0

Home > Wireless > Access Control Settings

Access Control Settings

Profile Name : RF Card A : VAP-1

Maximum Number of Clients : 128 *(Range: 1 ~ 256 per RF card)

Access Control Type : Disable Access Control

Maximum Number of Clients: The default policy is unlimited access without any authentication requirement. To restrict the station number of wireless connections, simply change the value to a desired number. For example, when the number of stations is set to 20, only 20 stations are allowed to connect to the specified VAP.

Access Control Type – Disable Access Control: When Disable is selected, there is no restriction for client devices to access the system.

Access Control Type – MAC ACL Allow List: When selecting *MAC ACL Allow List*, only the client devices (identified by their MAC addresses) listed in the Allow List (“allowed MAC addresses”) are granted access to the system. The administrator can temporarily block any allowed MAC address by checking *Disable*, until the administrator re-Enables the listed MAC.



Access Control Settings

Profile Name : RF Card A : VAP-1

Maximum Number of Clients : 32 *(Range: 1 ~ 256 per system)

Access Control Type : MAC ACL Allow List

No.	MAC Address	State
1		<input checked="" type="radio"/> Disable <input type="radio"/> Enable
2		<input checked="" type="radio"/> Disable <input type="radio"/> Enable
3		<input checked="" type="radio"/> Disable <input type="radio"/> Enable

►► Note:

An empty Allow List means that there is no allowed MAC address. Make sure at least the MAC of the management system is included (e.g. network administrator's computer)

Access Control Type – MAC ACL Deny List: When selecting *MAC ACL Deny List*, all client devices are granted access to the system except those listed in the Deny List (“denied MAC addresses”). The administrator can allow any denied MAC address to connect to the system temporarily by checking *Disable*.

Access Control Settings

Profile Name : RF Card A : VAP-1 ▼

Maximum Number of Clients : 32 *(Range: 1 ~ 256 per system)

Access Control Type : MAC ACL Deny List ▼

No.	MAC Address	State
1	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
2	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
3	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Access Control Type – RADIUS ACL: Authenticate incoming MAC addresses by an external RADIUS. When *RADIUS ACL* is selected, all incoming MAC addresses will be authenticated by an external RADIUS. Please note that each VAP's MAC ACL and its security type (shown on the **Security Settings** page) share the same RADIUS configuration.

Access Control Settings

Profile Name : RF Card A : VAP-1 ▼

Maximum Number of Clients : 32 *(Range: 1 ~ 256 per system)

Access Control Type : RADIUS ACL ▼

Primary RADIUS Server :

Note!!! These settings will also apply to security settings which use RADIUS Server for this VAP.

Host: *(Domain Name / IP Address)

Authentication Port: 1812 *(1 - 65535)

Secret Key: *

Secondary RADIUS Server :

Host:

Authentication Port:

Secret Key:

4.8 Hotspot 2.0

Hotspot 2.0 is also known as WiFi Certified Passpoint initiated by the WiFi Alliance to provide better bandwidth and services for public WiFi subscribers.

Status: Enable or Disable Hotspot 2.0

Internet Access: Enable if this network provides access to the internet

Access Network Type

- Private: Home and Enterprise Networks
- Private and Guest Access: Enterprises offering guest connectivity
- Chargeable Public Network: Available to all but requires a fee
- Free Public Network: Available to all without fees
- Personal Device Network: For peripherals in an ad-hoc mode
- Emergency Services
- Test/Experimental/Wild Card

Venue Information: The Group/Type of the venue is selected here. This identifies the general class of the venue and the specific type of venue within each Group.

Venue Name List: The Name of the Network Venue, which is useful to end users for network selection.

Network Authentication Type: The additional steps to acquire access for an unsecure network

- Acceptance of terms and conditions
- Online enrollment supported – may require user accounting
- HTTP/HTTPS redirection – the URL to which the browser is redirected is indicated
- DNS redirection – Note that the Hotspot 2.0 specification forbids network operators from supporting protocols that are not interoperable with DNSSEC. DNS redirection for captive portals violates this requirement.

Roaming Consortium Organizational Identifier: A roaming consortium is a group of service providers (SP) with which a user's credentials can be used for authentication. Roaming consortiums are identified by an organization identifier (OI) that is assigned by the IEEE—similar to the first half of a MAC address. An OI is often 24 bits in length, but can also be 36 bits (i.e. OUI-36).

IP Address Type: IPv4 or IPv6

NAI Realm List: An NAI Realm identifies the proper authentication server or domain for the user's authentication exchange. By discovering which authentication realms are supported by a network, a mobile device can selectively authenticate to its preferred networks.

- ECW Type – The NAI Realm list can also optionally indicate the Extensible Authentication Protocol (ECW) types supported by each realm as well as the authentication parameters for that ECW type.

Domain Name List: Lists one or more domain names for the entity operating the AP. This is a critical for Hotspot 2.0 network selection policy, as it identifies the operator of the network. It indicates to the mobile device whether they are at a home or visited Hotspot.

Cellular Network Information List (PLMN): Identifies the 3GPP cellular networks available through the AP. Specifically, this field identifies the Public Land Mobile Network (PLMN) ID, comprised of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the mobile operator.

Hotspot 2.0 R2 (Hotspot 2.0 Release 2): It includes improvements over Hotspot 2.0 Release 1. This feature only supports in ECW5211-L, ECW5410-L and ECWO5211-L.

- OSU SSID: the SSID name of the OSEN VAP
- OSU Server URI: the URI of the OSU server
- OSU Friendly Name: Name of the OSU provider in human language, which matches the name drawn from the OSU server certificate exactly. Now only support English
- OSU NAI: to authenticate to the OSU (if configured for OSEN)
- OSU Service Description: the description for the OSU. Now only support English

5. Firewall

The system provides an added security feature, Layer2 Firewall, in addition to the typical AP security. Layer2 Firewall offers a firewall function that is tailored specifically for Layer2 traffic, providing another choice of shield against possible security threats coming from/going to WLAN (AP interfaces); hence, besides firewall policies configured on gateways, this extra security feature will assist to mitigate possible security breach. This section provides information in the following functions: **Firewall Lists**, **Service** and **Advanced Firewall Settings**.

5.1 Firewall List

It provides an overview of firewall rules in the system; 6 default rules with up to a total of 20 firewall rules are available for configuration.



No.	State	Action	Name	EtherType	Remark	Setting
1	<input type="checkbox"/>	DROP	CDP	IEEE_8023		Del Ed In Mv
2	<input type="checkbox"/>	DROP	STP	IEEE_8023		Del Ed In Mv
3	<input type="checkbox"/>	DROP	GARP	IEEE_8023		Del Ed In Mv

From the overview table, each rule is designated with the following field;

No.: The numbering will decide the priority for the system to carry out the available firewall rules in the tables.

State: The check marks will enable the respective rules.

Action: **DROP** denotes a block rule; **ACCEPT** denotes a pass rule.

Name: Shows the name of the rule.

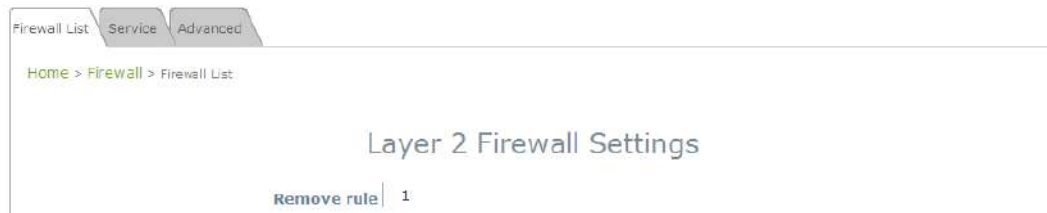
EtherType: Denotes the type of traffic subjected to this rule.

Remark: Shows the note of this rule.

Setting: 4 actions are available; **Del** denotes to delete the rule, **Ed** denotes to edit the rule, **In** denotes to insert a rule, and **Mv** denotes to move the rule.

To delete a specific rule,

Del in the Setting column of firewall list will lead to the following page for removal confirmation. After the **SAVE** button is clicked and system is rebooted, the rule will be removed.



To edit a specific rule,

Ed in the Setting column of the firewall list will lead to the following page for detail configuration. From this page, the rule can be edited from scratch or from an existing rule for revision. The following fields will be displayed:

Rule ID: The numbering of this specific rule will decide its priority among available firewall rules in the table.

Rule name: The rule name can be specified here.

EtherType: The drop-down list will provide the available types of traffic subjected to this rule.

Interface: It indicates inbound/outbound direction with desired interfaces.

Service (when EtherType is **IPv4**): Select the available upper layer protocols/services from the drop-down list.

DSAP/SSAP (when EtherType is **IEEE 802.3**): The value can be further specified for the fields in 802.2 LLC frame header.

Type (when EtherType is **IEEE802.3**): The field can be used to indicate the type of encapsulated traffic.

VLAN ID (when EtherType is **802.1 Q**): The VLAN ID is provided to associate with certain VLAN-tagging traffic.

Priority (when EtherType is **802.1 Q**): It denotes the priority level with associated VLAN traffic.

Encapsulated Type (when EtherType is **802.1 Q**): It can be used to indicate the type of encapsulated traffic.

Opcode (when EtherType is **ARP/RARP**): This list can be used to specify the ARP Opcode in ARP header.

Source: MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields.

Destination: MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields.

Action: The rule can be chosen to be **Block** or **Pass**.

Remark: Any note of this rule can be specified here.

When the configuration for firewall rule is completed; please click **SAVE** and **Reboot** system to let the firewall rule take effect.

To insert a specific rule,

In in the Setting column of the firewall list will lead to the following page for detail configuration with rule ID for the current inserted rule.

From this page, a rule can be added or edited from an existing rule for revision.

To move a specific rule,

Mv in the Setting column of the firewall list will lead to the following page for reordering confirmation.

After the **SAVE** button is clicked and system is rebooted, the order of rules will be updated.



Please make sure all desired rules (state of rule) are checked and saved in the overview page; the rules will be enforced upon system reboot.

Firewall List
Service
Advanced

Home > Firewall > Firewall List

Layer 2 Firewall Settings

Enable Layer 2 Firewall ☐ Disable ☒ Enable

No.	State	Action	Name	EtherType	Remark	Setting
1	<input checked="" type="checkbox"/>	DROP	CDP and VTP	IEEE_8023		Del Ed In Mv
2	<input type="checkbox"/>	DROP	STP/BPDU	IEEE_8023		Del Ed In Mv
3	<input type="checkbox"/>	DROP	GARP	IEEE_8023		Del Ed In Mv
4	<input type="checkbox"/>	DROP	RIP	IPv4		Del Ed In Mv
5	<input type="checkbox"/>	DROP	HSRP	IPv4		Del Ed In Mv
6	<input type="checkbox"/>	DROP	OSPF	IPv4		Del Ed In Mv
7	<input type="checkbox"/>					Del Ed In Mv
8	<input type="checkbox"/>					Del Ed In Mv
9	<input type="checkbox"/>					Del Ed In Mv
10	<input type="checkbox"/>					Del Ed In Mv

First Prev Next Last (total: 20)

SAVE

CLEAR

5.2 Service

The administrator can add or delete firewall services here; the services in this list will become options to choose in firewall rule (when EtherType is IPv4).

The Access Point provides a list of rules to block or pass traffic of layer-3 or above protocols. These services are available to choose from a drop-down list of layer2 firewall rule edit page with Ether Type IPv4. The first 28 entries are default services and the administrator can add/delete any extra desired services.

There are 28 firewall services available in default settings; these default services cannot be deleted but can be disabled. If changes are made, please click **SAVE** to save the settings before leaving this page.

Firewall ListServiceAdvanced

Home > Firewall > Service Config

Firewall Service

No.	Name	Description	Delete
1	ALL	ALL	<input type="checkbox"/>
2	ALL TCP	TCP, Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
3	ALL UDP	UDP, Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
4	ALL ICMP	ICMP	<input type="checkbox"/>
5	FTP	TCP/UDP, Destination Port: 20~21	<input type="checkbox"/>
6	HTTP	TCP/UDP, Destination Port: 80	<input type="checkbox"/>
7	HTTPS	TCP/UDP, Destination Port: 443	<input type="checkbox"/>
8	POP3	TCP, Destination Port: 110	<input type="checkbox"/>
9	SMTP	TCP, Destination Port: 25	<input type="checkbox"/>
10	DHCP	UDP, Destination Port: 67~68	<input type="checkbox"/>

First Prev Next Last (total: 28)

Add

5.3 Advanced

At **Firewall > Advanced**, more advanced settings on firewall rules can be configured, providing extra security enhancement against DHCP and ARP traffic traversing the available interfaces of the system.

Trust Interface: Each VAP interface can be checked individually to mark as trusted interfaces; security enforcements on DHCP/ARP like DHCP snooping and ARP inspection will be carried out on non-trusted interfaces.

DHCP Snooping: When enabled, DHCP packets will be validated against possible threats like DHCP starvation attack; in addition, the trusted DHCP server (IP/MAC) can be specified to prevent rouge DHCP server.

ARP Inspection: When enabled, ARP packets will be validated against ARP spoofing.

- **Proxy ARP** option when enabled, AP will reply ARP requests on behalf of downlink stations. The ARP table maintained by the AP will be used as a look up table upon receipt of ARP request from AP uplink. Adversely, without Proxy ARP, ARP request is broadcasted down into the AP's wireless network causing network inefficiencies.
- **Force DHCP** option when enabled, the AP only learns MAC/IP pair information through DHCP packets. Since devices configured with static IP address does not send DHCP traffic, any clients with static IP address will be blocked from internet access unless its MAC/IP pair is listed and enabled on the **Static Trust List**.
- **Trust List Broadcast** can be enabled to let other APs (with L2 firewall feature) learn the trusted MAC/IP pairs to issue ARP requests.
- **Static Trust List** can be used to add MAC or MAC/IP pairs of devices that are trusted to issue ARP request. Other network nodes can still send their ARP requests; however, if their IP appears on the static list (with different MAC), their ARP requests will be dropped to prevent eavesdropping.

RF Isolation (between RFs): Clients are isolated between RF Card A and RF Card B.

VAP Isolation (within RF): Clients on different VAPs on the same RF Card are isolated.

If any settings are changed, please click **SAVE** to save the configuration before leaving this page.

►► Note:

- RF Isolation (between RFs) may be limited on selected AP models.
- VAP Isolation (within RF) may be limited on selected AP model.

6. Utilities

The following utility features on this page allow the administrator to maintain the system: Change Password, Backup & Restore, System Upgrade, Reboot, Upload Certificate, Channel Analysis, Background Scan.

6.1 Change Password

To protect the Web Management Interface from unauthorized access, it is highly recommended to change the administrator's password to a secure password. Only alpha-numeric characters are allowed, and it is also recommended to make use of a combination of both numeric and alphabetic characters.



The screenshot shows the 'Utilities' tab selected in the top navigation bar. Below it, the 'Change Password' sub-tab is active. The page title is 'Change Password'. The breadcrumb trail is 'Home > Utilities > Change Password'. The form contains two sections for password changes:

- admin** section:
 - Name: admin
 - New Password: *up to 32 characters
 - Re-enter New Password:
- user** section:
 - Name: user
 - New Password: *up to 32 characters
 - Re-enter New Password:

The administrator can change password on this page. Enter the original password (“admin”) and new password, and then re-enter the new password in the **Re-enter New Password** field. Click **SAVE** to save the new password.

In addition to the admin account, there is a “user” account capable of accessing the web management interface with configuration limitations. The “user” account will not be able to reboot AP, change wireless settings or enable the Channel Analysis function. This account is typically issued by IT staff for employees to monitor AP statuses.

6.2 Backup & Restore

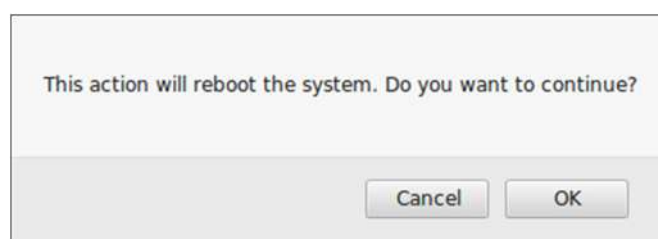
This function is used to backup and restore the Access Point's settings. The AP can also be restored to factory default using this function. It can be used to duplicate settings to other access points (backup settings of this system and then restore on another AP).



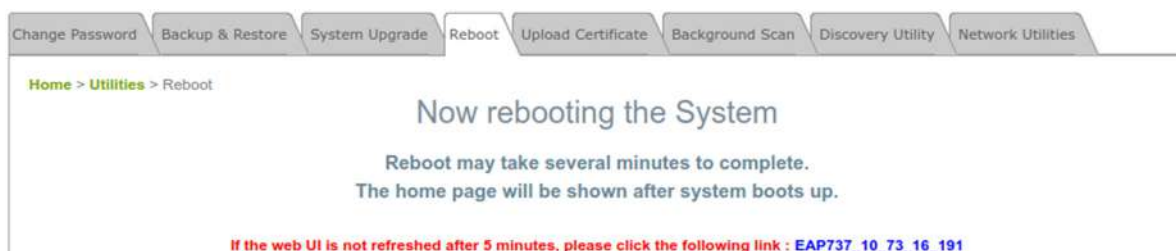
Reset to Default

Typically, administrators can reset the system to factory default from the Web Management Interface as below description. Additionally, there is another way to from the Console Interface and just refer to *"session 8.2 Remote Connection by SSH Interface"*

- **Keep Network Interface Settings:** in some cases, it is helpful to check this option to ensure the original Network Interface settings remain even after a system reset-to-default.
- **Keep VLAN for Management:** in some cases, it is helpful to check this option to ensure the original VLAN for Management settings remain even after a system reset-to-default.
- Click **Reset** to load the factory default settings. A pop-up message will appear to re-confirm the request to reboot the system. Click **OK** to proceed, or click **Cancel** to cancel the action.



- A message as displayed below will appear during the reboot period. The system power must be kept on before the completion of the reboot process. The **System Overview** page will appear upon reboot completion.



Backup System Settings: to save the current system configurations to a backup file on a local disk of the management console. A backup file can be restored to the system by clicking **Choose File** button to select the backup file and then clicking **Restore** button to execute the process.

Restore System Settings: to click **Choose File** to search for a .db database backup file created by the controller and click **Restore** to restore to the same settings at the time when the backup file was saved.

6.3 System Upgrade

There are two methods of firmware upgrade: via the WMI or via a TFTP server. The administrator can obtain the latest firmware from the Edgecore Support Team. To upgrade the firmware, click “Choose File” to select the new firmware file you downloaded onto your PC and then click “Upload” to execute the process. To upgrade by TFTP, enter the designated IP address, Port, and File Name, then click “Apply”. Please restart the system after upgrading the firmware.

►► Note:

- It is recommended to check the firmware version number before proceeding further. Please make sure you have the correct firmware file.
- Firmware upgrade may sometimes result in the loss of data. Please ensure that all necessary settings are written down before upgrading the firmware.
- During firmware upgrade, please do not turn off the power. This may permanently damage the system.
- Upgrade by TFTP may be limited on selected AP models.

6.4 Reboot

Click **Reboot** to restart the AP safely. The process takes approximately three minutes. The System Overview page will appear after a successful reboot. Note: in some cases, it is necessary to reboot the AP to ensure that parameter changes are submitted.



6.5 Upload Certificate

This function is used to configure a valid certificate for security validation required in CAPWAP.

Home > Utilities > Upload Certificate

Upload Certificate

Upload Private Key	
File Name	<input type="text"/> <input type="button" value="Browse..."/>

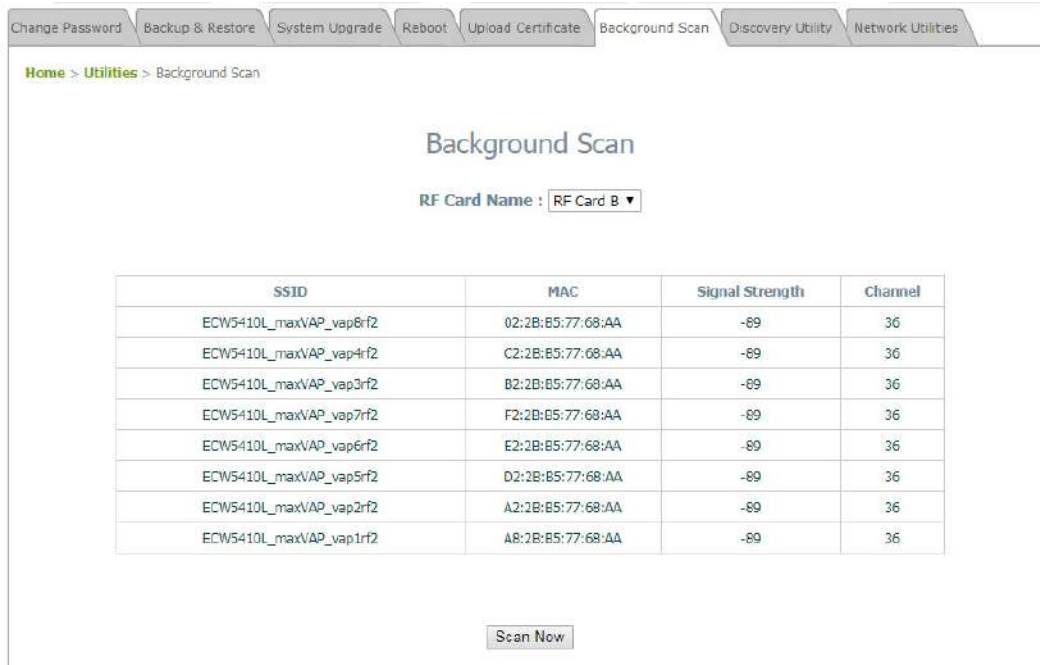
Upload Certificate	
File Name	<input type="text"/> <input type="button" value="Browse..."/>

Upload Trusted Certificate	
File Name	<input type="text"/> <input type="button" value="Browse..."/>

- **Upload Certificate:** It provides flexibility to support customer's own Certificate, Private Key, or Trusted Certificate for a means of security verification for CAPWAP or other security needs to ensure the authenticity of this AP to other network entities.
- **Use Default Certificate:** Click *Use Default Certificate* to use the default certificate and key.

6.6 Background Scan

The Access Point is capable of doing background scanning without affecting service. This works in complement with Channel Analysis so administrators have a complete overview of the wireless environment.



Background Scan

RF Card Name : RF Card B ▼

SSID	MAC	Signal Strength	Channel
ECW5410L_maxVAP_vap8rf2	02:2B:85:77:68:AA	-89	36
ECW5410L_maxVAP_vap4rf2	C2:2B:85:77:68:AA	-89	36
ECW5410L_maxVAP_vap3rf2	B2:2B:85:77:68:AA	-89	36
ECW5410L_maxVAP_vap7rf2	F2:2B:85:77:68:AA	-89	36
ECW5410L_maxVAP_vap6rf2	E2:2B:85:77:68:AA	-89	36
ECW5410L_maxVAP_vap5rf2	D2:2B:85:77:68:AA	-89	36
ECW5410L_maxVAP_vap2rf2	A2:2B:85:77:68:AA	-89	36
ECW5410L_maxVAP_vap1rf2	AB:2B:85:77:68:AA	-89	36

Scan Now

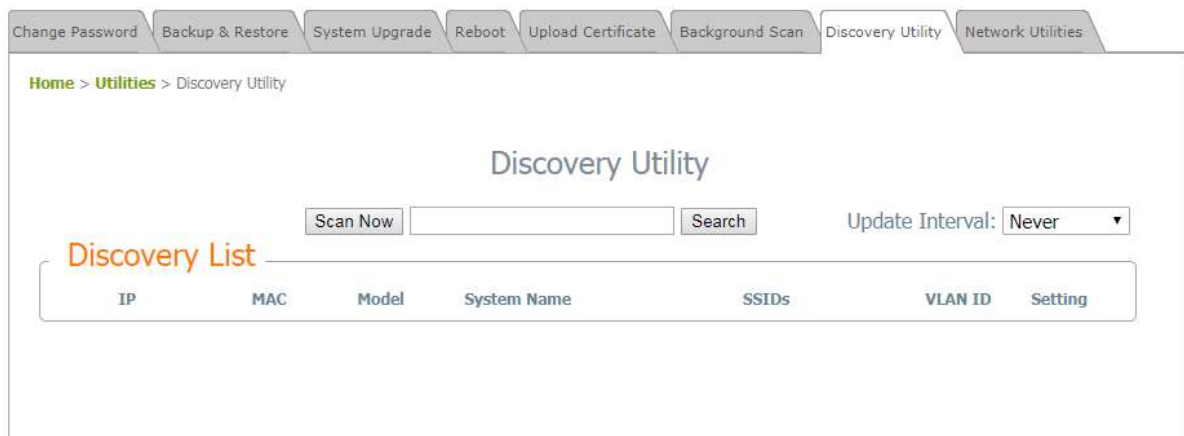
The Scan Whole Channel button triggers the AP to scan all channels in the configured band. Note that the Radio is only capable of scanning in its configured band.

6.7 Discovery Utility

The network administrators need to access or change some information without entering AP interface, such as forget the IP address of the AP, forget the admin's password, or configure the IP address of the AP.

All they need to do is connect Edgecore AP within the same Layer 2 from the ports of the current system, and press the "Search" button to execute the IP Discovery Utilities. The scanning results would be devices' corresponding IP address, MAC address, Model, System Name, SSID (each VAP), VLAN ID. The LAN ports of devices could connect through switch to other devices (APs).

This powerful and proprietary built-in utility is now both in WHG and ECW/ECWO series.



Scan Now: Click this button to start the discovery process, and the results will be displayed in the Discovery List table.

Search: Enter a keyword to search for the particular AP(s).

Change: This allows administrators to change the particular AP's settings, including IP address, Netmask, Gateway, Primary DNS Server, Username, and Password.

6.8 Network Utilities

Ping: It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not.

Trace Route: It allows administrator to recover the real path of packets from the gateway to a destination using IP address or Host domain name.

ARPing: Allows the administrator to send ARP request for a specific IP address or domain name.

Result: The operation result is displayed here.

The screenshot shows the 'Network Utilities' section of a web interface. At the top, there is a navigation bar with tabs: Change Password, Backup & Restore, System Upgrade, Reboot, Upload Certificate, Background Scan, Discovery Utility, and Network Utilities. Below the navigation bar, the breadcrumb trail is 'Home > Utilities > Network Utilities'. The main heading is 'Network Utilities'. There are three input sections: 'Ping (Domain/IP):' with the value '8.8.8.8' and a 'Ping' button; 'Trace Route:' with an empty input field and 'Start' and 'Stop' buttons; and 'ARPing:' with an empty input field and an 'ARPing' button. Below these sections, the results of the ping test are displayed in a text box. The results show five successful ping attempts to 8.8.8.8, each with 56 data bytes and response times ranging from 2.903 ms to 3.853 ms. The statistics summary indicates 5 packets transmitted, 5 packets received, 0% packet loss, and a round-trip time range of 2.903/3.415/3.853 ms.

```

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=58 time=3.853 ms
64 bytes from 8.8.8.8: seq=1 ttl=58 time=2.903 ms
64 bytes from 8.8.8.8: seq=2 ttl=58 time=3.250 ms
64 bytes from 8.8.8.8: seq=3 ttl=58 time=3.688 ms
64 bytes from 8.8.8.8: seq=4 ttl=58 time=3.385 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.903/3.415/3.853 ms
  
```

7. Status


The following function tabs present the current condition and state of the system: Overview, Interfaces, Associated Clients, DHCP Lease, Link Status, Event Log, Wireless Log, and Monitor.

7.1 Overview

The **System Overview** page provides an overview of the system status for the administrator.


[Home](#) > [Status](#) > System Overview

System Overview




System

System Name	ECW5410-L
Firmware Version	3.43.00
Build Number	1.55-1.9293.2.21
Location	
Site	EN-A
Device Time	2009/01/03 00:59:23
System Up Time	2 days, 1:00:20
CPU/RAM Usage	3.19% / 35.00% Plot




Radio Status

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	A8:2B:B5:77:68:61	802.11g+n	6	18 dBm
RF Card B	A8:2B:B5:77:68:62	802.11ac	36	19 dBm




LAN Interface


MAC Address	A8:2B:B5:77:68:5F
IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Gateway	192.168.1.254



AP Status


RF Card Name: RF Card A

Profile Name	BSSID	ESSID	Security Type	Online Clients	TUN
VAP-1	A8:2B:B5:77:68:61	Guest Network	Open	0	



CAPWAP

Status: Disabled

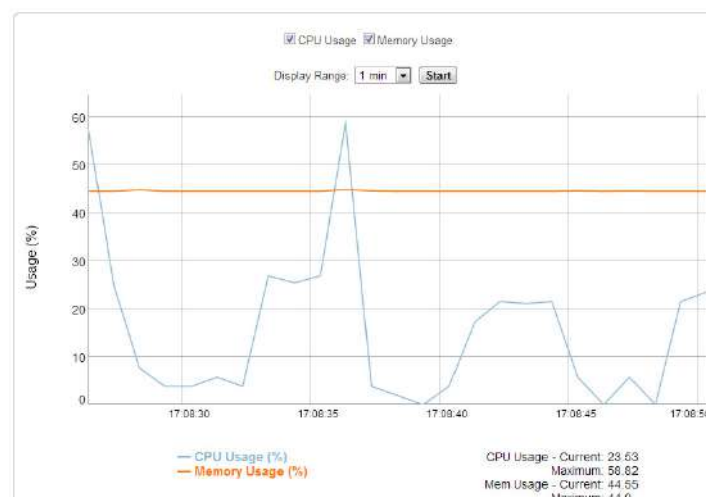


IPv6

Status: Disabled

Clicking **Plot** button shows the real time plot of CPU/RAM usage. Left click and drag the mouse to zoom in the desired regions. Double click on the graph to return the plot to its original scale.:

CPU / Memory Usage



7.2 Interfaces

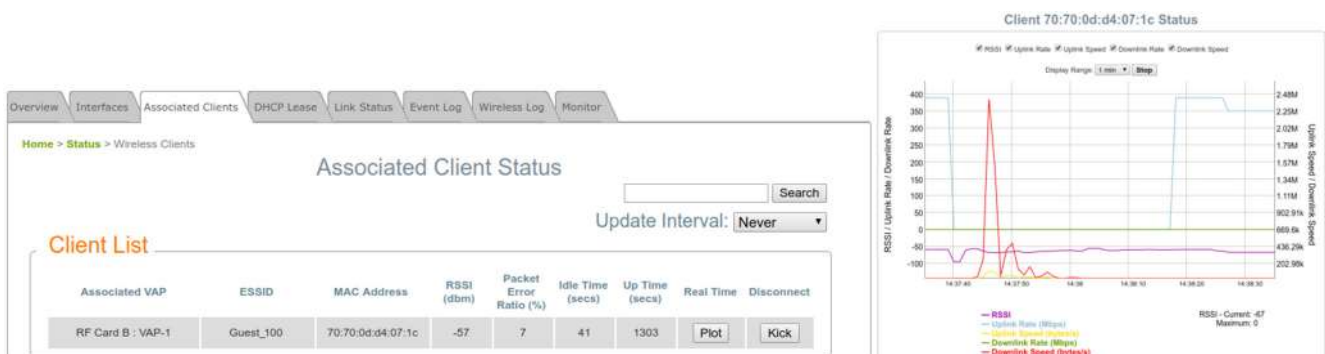
Traffic information is available per interface. Recorded data includes **Packets In**, **Packets Out**, **Traffic In (kb)**, and **Traffic Out (kb)**.



A real time plot is also available for each interface, whose time axis is configurable with the following options: 1 minute, 2 minutes, 5 minutes, or 10 minutes. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

7.3 Associated Clients

The administrator can remotely oversee the status of all associated clients on this page. When a low SNR is found here, the administrator can tune the corresponding parameters or investigate the settings of associated clients to improve network communication performance.



A real time plot is also available for each interface, whose time axis is configurable with the following options: 1 minute, 2 minutes, 5 minutes, or 10 minutes. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

Associated VAP: The name of the VAP that the client is associated with.

ESSID: The Extended Service Set ID which the client is associated with.

MAC Address: The MAC address of associated clients.

RSSI: The Received Signal Sensitivity Index of respective client's association.

Packet Error Ratio: Indication of the associated client's service quality to see if packets are not received.

Idle Time: Time period that the associated client is inactive for; the time unit is in seconds.

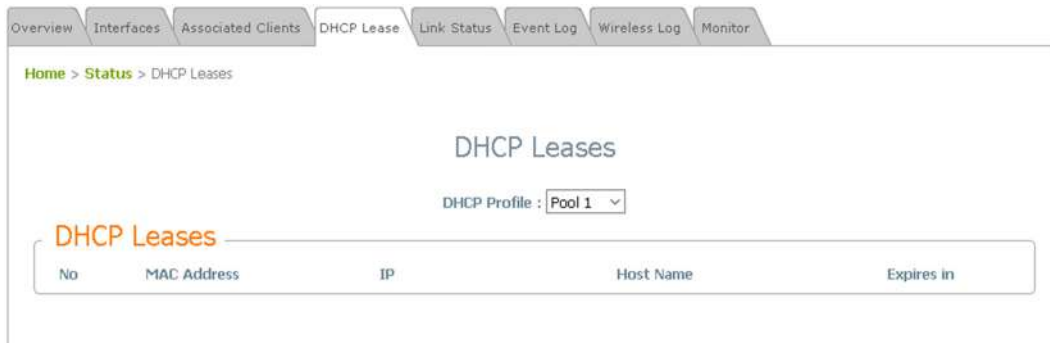
Up time: Time period that the client is associated for; the time unit is in seconds.

Real Time (Plot): A real time plot of each associated client's traffic information including Packets In/Out, Traffic In/Out in Kb, RSSI, Uplink/Downlink Rates, and etc.

Disconnect: Upon clicking *Kick*, the client will be disconnected from the system.

7.4 DHCP Leases

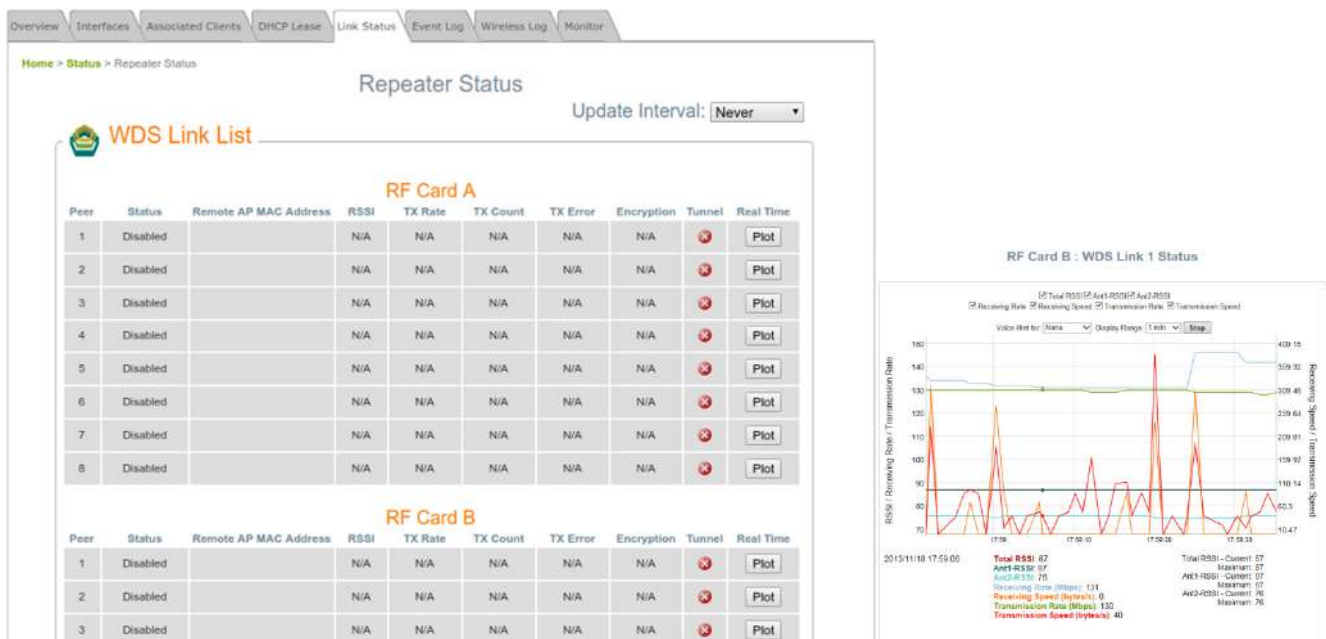
When any VAP operates in NAT mode, DHCP Lease information will be displayed in this table.



7.5 Link Status

The administrator can review detailed information of the repeater function at **Status > Link Status**.

Information of WDS status, traffic statistics, encryption and other details are provided.



By clicking plot, a dynamic graph for WDS link status is displayed. Information on the plot includes Total RSSI, Ant1 RSSI, Ant2 RSSI, Transmission Rate, Receiving Rate, Transmission Speed, and Receiving Speed.

A real time plot is also available for each interface, whose time axis is configurable with the following options: 1 minute, 2 minutes, 5 minutes, or 10 minutes. Double click to return the plot to its original scale.

Voice hint may also be enabled for convenience during antenna adjustment.

7.6 Event Log

The Event Log provides a record of system event. Administrators can monitor the system status by checking this log. Internal storage is limited so it is recommended to back up all logs via an external Syslog Server.



Each entry in the Event Log represents an event record; in each line, there are 4 fields:

Date and Time: The time and date when the event happened.

IP Address: to indicate which LAN IP address of the system recorded this event. Note that all events on this page are local events, so the IP address in this field is always the same. In remote SYSLOG service however, this field will help the administrator identify which event is from this Access Point.

Process name: to indicate the event generated by the running instance

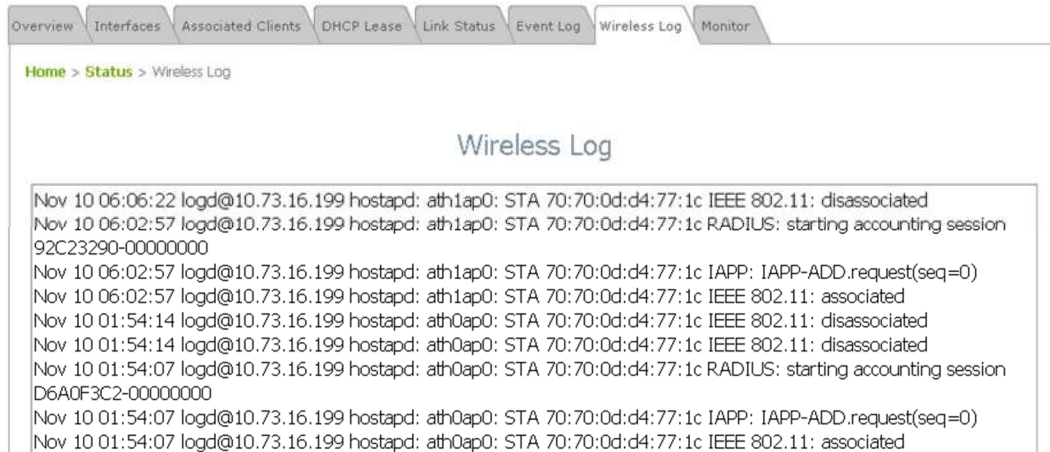
Description: to display the message of each event

SAVE LOG: to save the file to local disk as a .txt file

CLEAR: to clear all of the records

7.7 Wireless Log

This Wireless Log keeps track of client association and WDS connection related activities. Administrators can monitor the system status by checking this log. Internal storage is limited so it is recommended to back up all logs via an external Syslog Server.



Each entry in the Wireless Log represents an event record; in each line, there are 4 fields:

Date and Time: The time and date when the event happened.

IP Address: to indicate which LAN IP address of the system recorded this event. Note that all events on this page are local events, so the IP address in this field is always the same. In remote SYSLOG service however, this field will help the administrator identify which event is from this Access Point.

Process name: to indicate the event generated by the running instance

Description: to display the message of each event

SAVE LOG: to save the file to local disk as a .txt file

CLEAR: to clear all of the records

7.8 Monitor

Multiple monitor charts provide a quick overview on the AP's performance in time dimension. Begin and End time for each chart can be selected for filtering data. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

CPU and Memory: to view the usage of the devices. CPU < 90% and RAM < 90% is acceptable

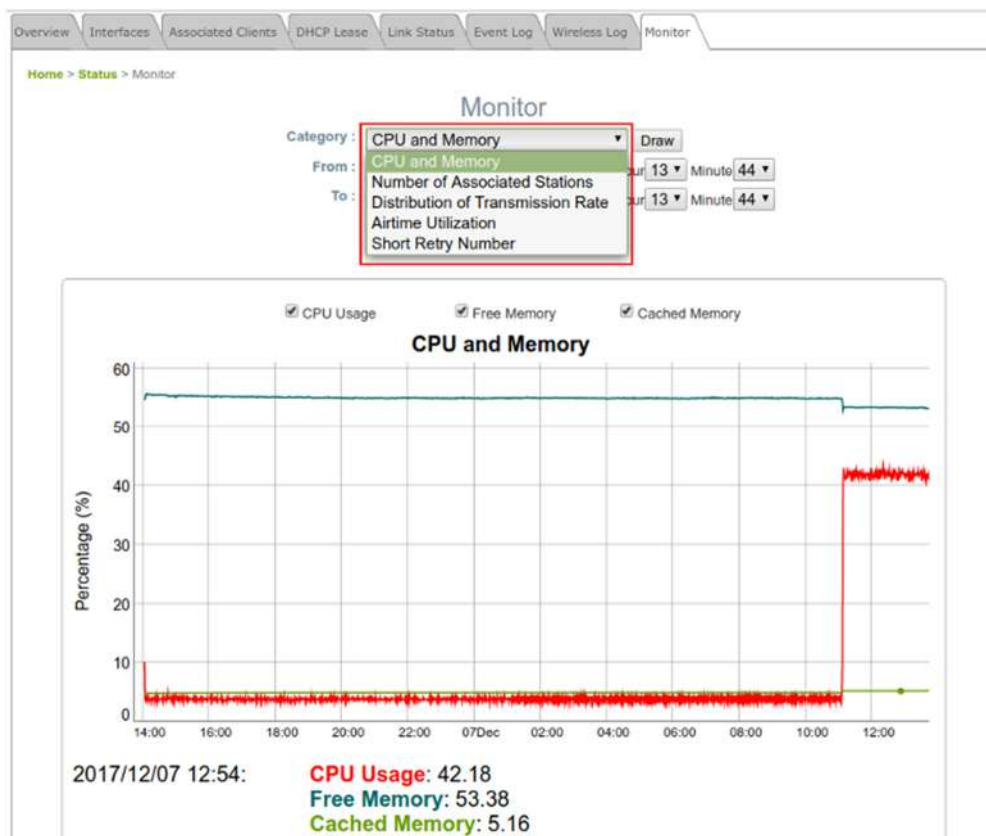
Number of Associated Station: to view the number of devices connected to the selected radio (RF Card A or RF Card B).

Distribution of Transmission Rate: to view the number of packets transmitted categorized by Transmission Rates.

Airtime Utilization: to view the Signal-to-Noise of the Wireless Environment. Airtime Utilization < 70% is optimal

- **RX Clear Rate:** The percentage of the airtime the current channel utilizes.
- **RX Frame Rate:** The percentage of airtime that the AP receives and decrypts.
- **TX Frame Rate:** The percentage of airtime from the AP transmitting data.

Short Retries Number: to view the number of packets re-transmitted. Short Retry < 200 is optimal





8. Console Interface

Via the console port, administrators are able to enter the console interface to reset the AP to its factory default settings. In order to connect to the console port of a The AP, a console cable, and a terminal simulation program (e.g. PuTTY) are needed. There are 2 ways to access the console interface.

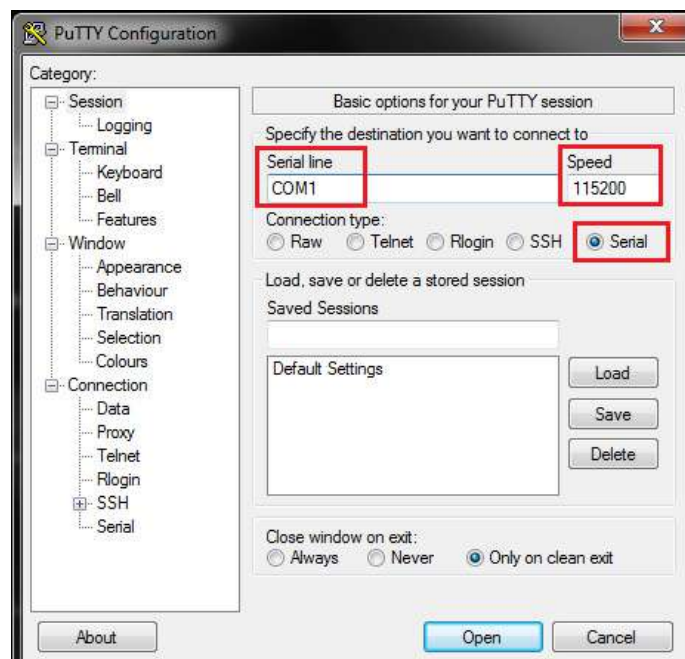
8.1 Direct Connection by Console Cables

PC > USB to RS-232 DB9 Serial Converter Cable > Console Cable (DB9-to-RJ45) > Console Port

The USB-to-RS232 cable is not supplied with standard packaging. It is recommended to use only the console cable provided with the packaging.

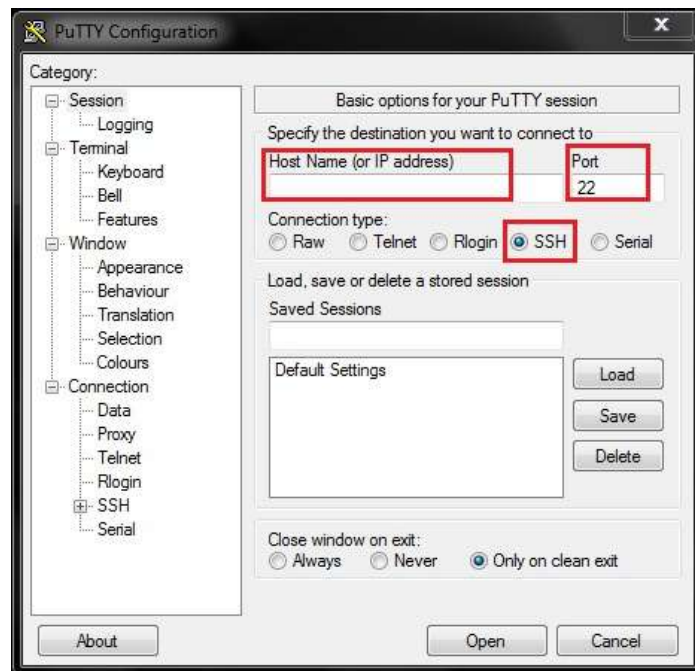
Cable	Description
	USB to RS-232 Serial Converter Cable (USB to DB9 Male)
	Console Cable (DB9 Female to RJ45 Male)

The speed (baud rate) is 115200.

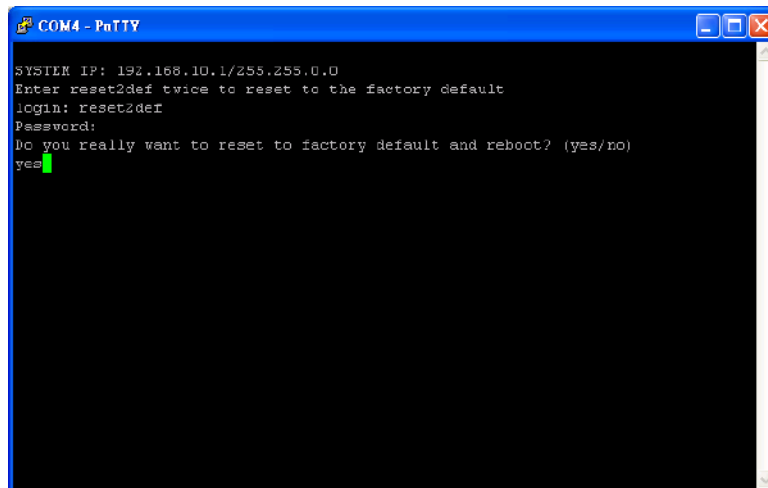


8.2 Remote Connection by SSH Interface

The system supports access to the console interface via SSH. Typically SSH utilizes Port 22 and would require the WAN IP address for access.



To reset the system to factory default through the console interface, Login as “reset2def” and enter “reset2def” as your password.




If the console connection is not readily available, the IP address of the AP can be retrieved with the Discovery Utility of another AP (Home > Utilities > Discovery Utility). Simply connect via an Ethernet cable and run the Discovery Utility.

9. Hardware Overview

ECW5210-L



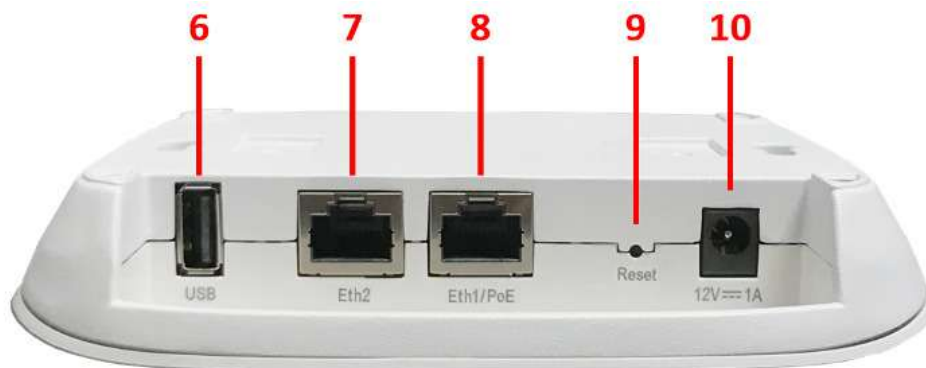
1	LED Indicators	An LED indicator is available to show the uplink status
2	12V  2.5 A	Attach power adaptor here
3	Uplink (PoE) Port	Offers uplink connection. This port can be used to connect to a controller, gateway, or directly to the Internet. 802.3at PoE is also supported



ECW5211-L

Front View



Side View



No.	Item Name	Description
1	 LED	<p>Power / Status LED Indicator:</p> <p>(a) Steady green light indicates a proper connection to a power source and normal operation.</p> <p>(b) The LED Indicator will start blinking when the Reset button is pressed:</p> <p>(b1) if pressed and hold for less than 5 seconds - the LED will blink slowly, indicating that the AP is restarting.</p> <p>(b2) if pressed and hold for more than 5 seconds - the LED will blink slowly for the first 5 seconds and then blink quickly, indicating the AP is resetting to factory default settings and restarting.</p>
2	2G-WiFi LED	2.4 GHz Wi-Fi LED Indicator: blinking indicates that the AP is sending or receiving traffic on 2.4 GHz band.
3	5G-WiFi LED	5 GHz Wi-Fi LED Indicator: blinking indicates that the AP is sending or receiving traffic on 5 GHz band.
4	Eth1/PoE LED	Eth1/PoE port status LED Indicator: turned on when traffic is passing through Eth1/PoE port.
5	Eth2 LED	Eth2 port status LED Indicator: turned on when traffic is passing through Eth2 port.
6	USB Port	USB interface reserved for future use.
7	Eth2 Port	RJ-45 port for Ethernet connection with downlink devices.
8	Eth1/PoE Port	RJ-45 port for uplink Ethernet connection and for PoE in. It is the default port that can pass all VLAN traffic to an uplink device (e.g. VLAN switch).
9	Reset Button	Press and release the button quickly (for less than 5 seconds) to restart the AP; to reset the AP to factory default settings, press & hold it for more than 5 seconds.
10	12V  1 A	The power socket to attach the power adapter.

ECW5410-L

Front View




Side View



Side View



1	Power LED	ECW5410-L status. The Status LED will start blinking when the restart/reset button is pressed. For the first 5 seconds, the LED will blink slowly (restart), and after 5 seconds, the LED will start blinking quickly (reset).
2	2.4G LED	2.4G Wi-Fi status. The 2.4G LED will blink when there is 2.4G traffic.
3	5G LED	5G Wi-Fi status. The 5G LED will blink when there is 5G traffic.
4	Uplink LED	Uplink status. The Uplink LED will light up when there is traffic passing through the Uplink port.
5	LAN LED	LAN status. The LAN LED will light up when there is traffic passing through the LAN port.
6	12V  2 A	Attach power adaptor here.
7	Uplink (PoE) Port	Offers uplink connection. This port can be used to connect to a controller, gateway, or directly to the Internet. 802.3af PoE is also supported.
8	LAN Port	The ports for connections with LAN side devices.
9	Console Port	To access ECW5410-L via the console interface.
10	Restart / Reset	Press once to restart the system; to reset the system to factory default settings, hold for more than 5 seconds.
11	USB Port	USB interface reserved for future use.

ECWO5210-L

Top View



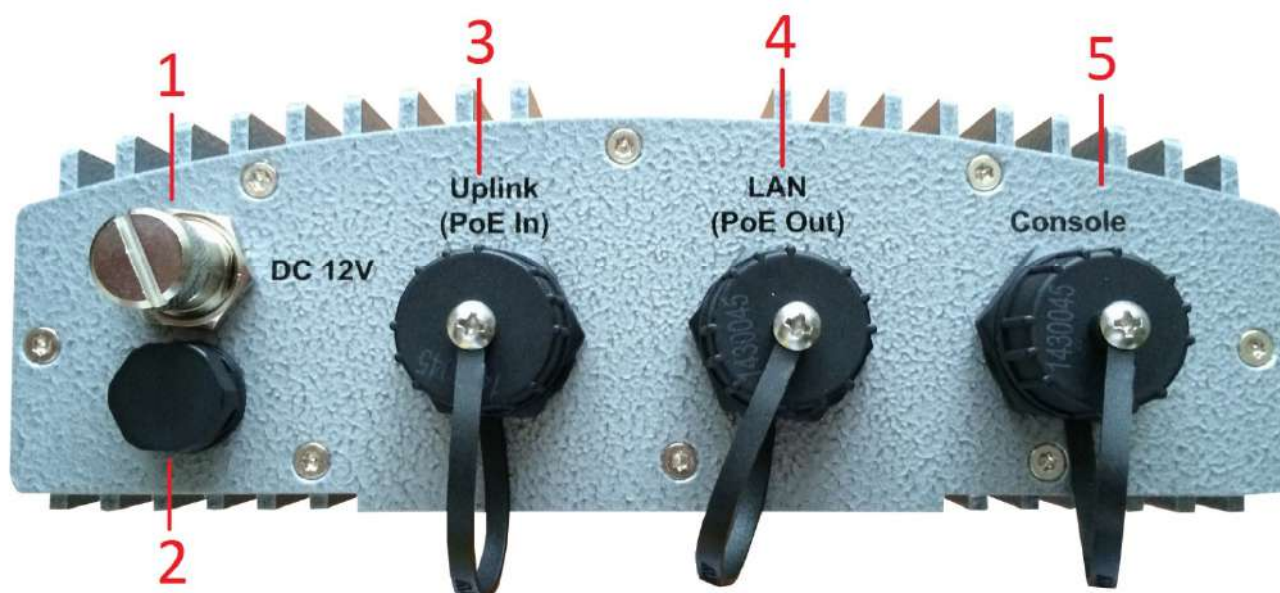
N-type Connector x 6	<p>For connecting to an antenna (RF Card A x 3, RF Card B x 3)</p> <p>Connector marked –1 is for the primary antenna when the AP is not in 802.11n or 802.11ac mode. Utilize all connectors for optimized MIMO performance.</p>
----------------------	---

Back View



Ground Connector	For connecting the ground wire
------------------	--------------------------------

Bottom View

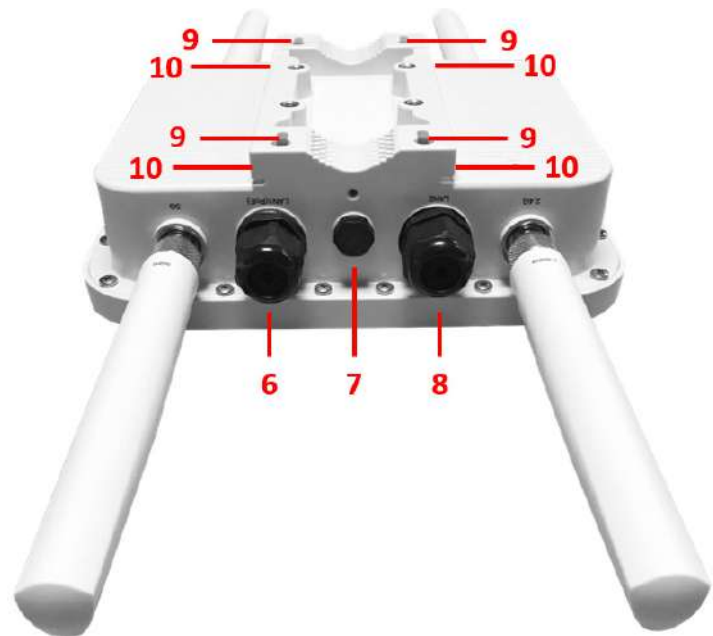


1	M12 DC Connector	DC input (12V) is supported on ECWO5210-L
2	Ventilation Valve	Due to extreme weather conditions, water vapor in the ECWO5210-L may condense. The valve allows ventilation to prevent moisture buildup within the ECWO5210-L.
3	Uplink (PoE Connector)	For connecting to the Power Sourcing Equipment (PSE)
4	Ethernet LAN	Attach Ethernet cables here for connecting to the wired local network
5	Console	The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft's Hyper Terminal for troubleshooting purposes.

ECWO5211-L



Side View



Back View

1	Power LED	ECWO5211-L status. The Power LED will start blinking when the ECWO5211-L is booting. After finishing booting, the Power LED will always on.
2	LAN1 LED	Uplink status. The LAN1 LED will light up when there is traffic passing through the LAN1 port.
3	LAN2 LED	LAN status. The LAN LED will light up when there is traffic passing through the LAN port.

4	2.4G LED	2.4G Wi-Fi status. The 2.4G LED will blink when there is 2.4G traffic.
5	5G LED	5G Wi-Fi status. The 5G LED will blink when there is 5G traffic.
6	LAN1 (PoE) Port	Offers uplink connection. This port can be used to connect to a controller, gateway, or directly to the Internet. 802.3at PoE is also supported.
7	Ventilation Valve	Due to extreme weather conditions, water vapor in the ECWO5211-L may condense. The valve allows ventilation to prevent moisture buildup within the ECWO5211-L.
8	LAN2 Port	The ports for connections with LAN side devices.
9	Wall Mounting Holes	For hanging ECWO5211-L.
10	Pole Mounting Gap	For mounting ECWO5211-L.

P/N: V34300171213